

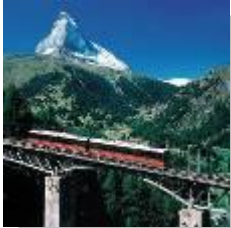


**InfoGuard Network Encryption**

**GSE Garderen  
28 October 2009**

**Optical encryption is critical –  
how safe is your core network?**





- **InfoGuard**
  - Your Partner for Security. Made in Switzerland!
  
- **High-speed Networking**
  - The Challenge in MAN-, WAN- and SAN-Networks
  - Security Myths and Realities
  
- **High Performance Encryption Solution**
  - 1/10 Gbps Ethernet-Encryption
  - 20 Mbps – 1 Gbps Multipoint Ethernet-Encryption
  - OC-192/STM-64 Data Encryption
  - 10 Port Multilink and Multiprotocol Encryption for Ethernet, Fibre Channel and FICON connections



# InfoGuard – security requires specialists



InfoGuard AG  
Zug / Switzerland

- Member of the Swiss «The Crypto Group» with more than 300 security experts
  - Own development and in-house-production of ICT-security solutions since 1952
  - Customers in 130 countries worldwide



# Industrial Espionage is a fact

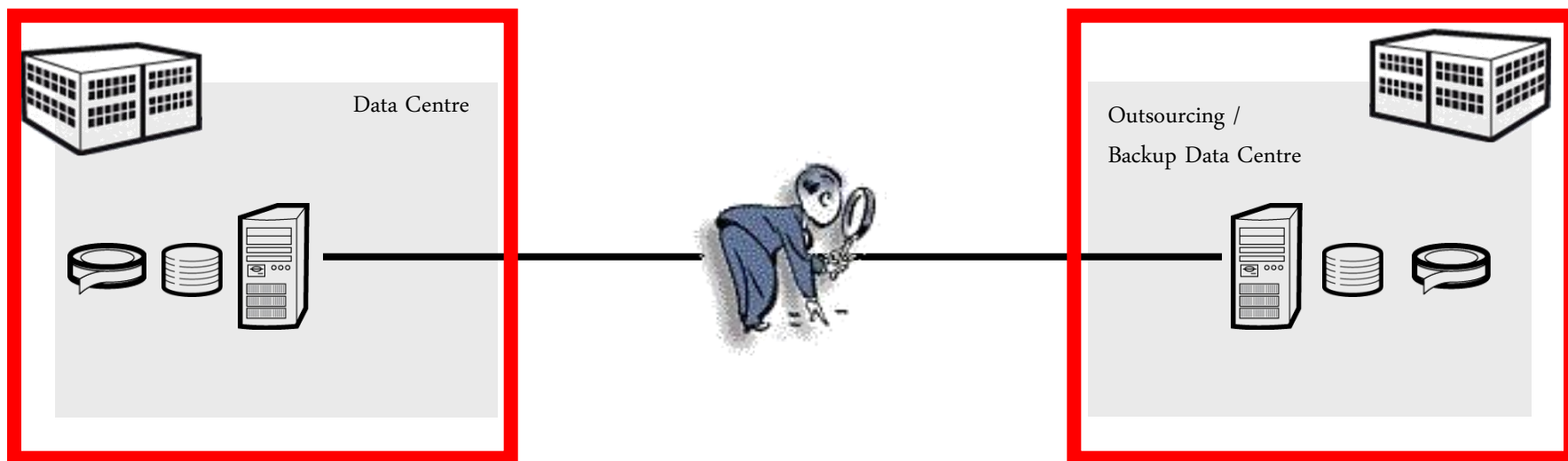


- **59% of breaches caused through HACKING!**
- **Payment card industry – 84% (Type of data)**
- **75 percent of breaches were not discovered by the victim**
- **73 percent of data breaches were caused by external parties**

Source: **Verizon's 2008 DATA BREACH INVESTIGATIONS REPORT**



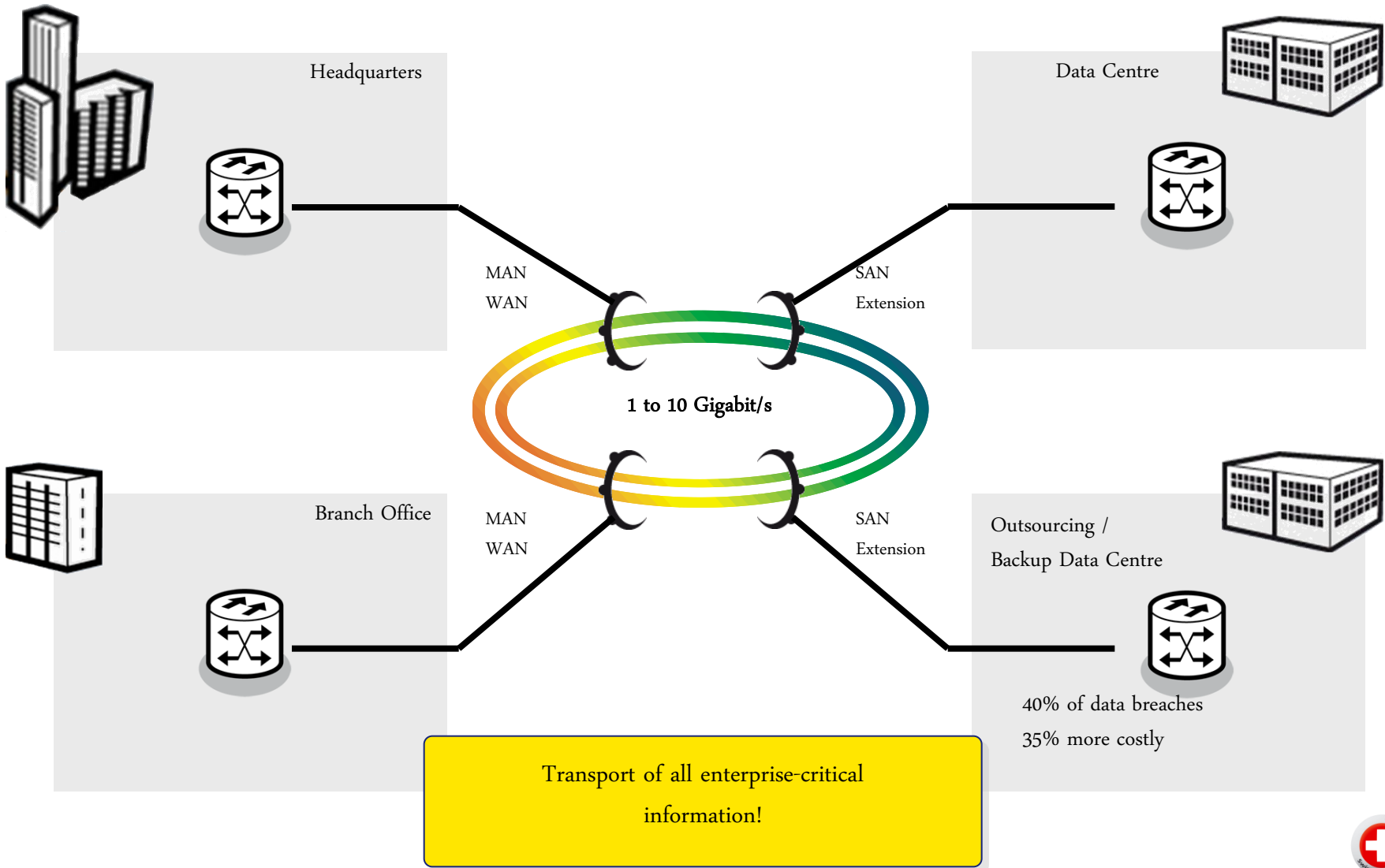
# High-speed Networking Data Centre Security



- Highest physical security
- Access to System and Processes
- Automated building access controls
- Onsite security staff
- Intrusion Detection System and Camera surveillance
- Fire protection system and gas extinguishers
- High availability of data centre connections, infrastructures and the supply of electric power



# High-speed Networking – Backbone of an enterprise



# Fibre optic networks – new target for economic espionage



*“Tapping a fiber-optic cable without being detected,  
and making sense of the information you collect,  
isn’t trivial but has certainly been done by **intelligence  
agencies** for the past **seven or eight years**. **These days,**  
it is within the range of a **well-funded hacker ...**”*

John Pescatore, VP of Security Gartner Group and former NSA analyst



*“... **our advice** to enterprises is to use **encryption** over  
all network connections where the physical security of access to the network, whether  
**copper or fibre or wireless**, cannot be secured ”*





## TECHNOLOGY ASSESSMENT

### Fiber-Optic Networks: Is Safety Just an Optical Illusion?

Romain Fouchereau

IDC specialist in firewall/VPN, IDS/IPS, and unified threat management

- "...there is an urgent need for government bodies to regulate on the security issues posed by fiber-optic networks."
- "...securing the inside network is not sufficient enough, data going from one site to the other can be intercepted and this security gap needs to be addressed."
- "...the only real preventive solution to protect information is to encrypt the data before it goes through the network."

Available to the public at [www.IDC.com](http://www.IDC.com) or via [http://www.infoguard.com/docs/PDF/IDC\\_report\\_Fibre\\_optic\\_security.pdf](http://www.infoguard.com/docs/PDF/IDC_report_Fibre_optic_security.pdf)



# Fibre optic networks – a profitable target for industrial espionage



Tapping of information - and data-networks are **seldom discovered** here are some published examples of optical breaches:

- Security forces in the US discovered an illegally installed fibre eavesdropping device in **Verizon's optical** network. It was placed at a mutual fund company.....shortly before the release of their quarterly numbers
- US Government have set up **secret rooms AT&T** (WorldNet) and have eavesdropping capability to worldwide networks
- French monitors on UK wireless networks for tapping top-level-management-conversations in **bidding processes**
- Criminals illegally monitoring **Dutch and German police** networks
- Networks of **pharmaceutical giants** in the U.K. and France
- Tapping of the **optical networks** between the (former) FRG and West-Berlin, installed by the GDR secret service STASI
- Three main trunk lines of **Deutsche Telekom** were breached at Frankfurt Airport in Germany



**More and more information is being lost**

US: In over 40 states now it is mandatory to disclose a security breach

# Thieves hack 4.2million credit and debit card details from PCI compliant Hannaford Supermarket chain!



- 1800 reported cases of fraud have resulted so far
- Breach undiscovered for 3 months and took a further 10 days to contain.
- 30 US secret servicemen, forensics experts and information technologists took more than 10 days of round-the-clock troubleshooting
- Apparently hackers had tapped 'state-of-the-art' fibre-optic cable that "security experts had believed was secure".
- **Avivah Litan**, a security and fraud analyst with **Gartner Inc.** states: 'attackers increasingly are going after the data in transit, ... not well-specified in the payment card standards.'
- If your network isn't properly segmented, and payment card information is sent in the clear over internal networks, **it's game over** if there's a crooked insider in your midst, said **John Nicholson**, a senior associate at **Pillsbury Winthrop Shaw Pittman LLP**.



WSJ March 2008



# Theft ring accused of hacking 41 million credit card numbers



- **Eleven people**, including a U.S. Secret Service informant, have been charged (U.S. citizens, Estonia, Ukraine, Belarus and China).
- Total dollar amount lost: "**impossible to quantify at this point.**" Attorney General Michael Mukasey
- Suspects **hacked into the wireless computer networks** of retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW and **set up programs that captured card numbers, passwords and account information.**
- "They used **sophisticated computer hacking techniques** that would allow them to breach security systems and install programs that gathered **enormous quantities of personal financial data**, which they then allegedly either sold to others or used themselves," Attorney General Michael Mukasey said at a news conference.
- alleged ringleader Albert (Segvec) Gonzalez of Miami was charged with **computer fraud, wire fraud, access device fraud, aggravated identity theft and conspiracy.** Now in custody in New York, he faces a maximum penalty of **life in prison** if convicted of all the charges.



StarTribune August 08





- **Basel II**
  - Ensures appropriate capital allocation according to a financial institutions: Market – Credit – Operational risk (*loss resulting from inadequate or failed internal processes, people or systems*)
- **EC Directive 2002/58/ Data Protection Act 1998, EU**
  - Stipulates **appropriate technical and organizational means** to protect against unauthorized access or processing of private data.
- **Payment Card Industry Security Standard-PCI**
  - applies to all members, Merchants and service providers that store, process or transmit cardholder data.  
**Requirement 4:**  
**Encrypt transmission of cardholder data across open, public networks**
- **Others** referring specifically to encryption as a requirement
  - **CA-SB** California SB 1386 – disclose of security breaches – unless encrypted – now law in 43 states
  - **HIPAA** Health Insurance Portability and Accountability Act of 1996



# Data encryption in fibre optical networks as 'Best Practice'



- *"Credit Suisse considers encryption of data in fibre optic networks – a crucial part of their security strategy – as an urgent obligation. The products of InfoGuard achieve all important requirements: High performance without significant latency and economical operation with lowest demands on maintenance."*

Jürg Frei,

Manager Networks Switzerland and  
Responsible for Strategy and Transformation of  
Global Networks



# Fibre optic networks – Security Myths!



Myth Loch Ness

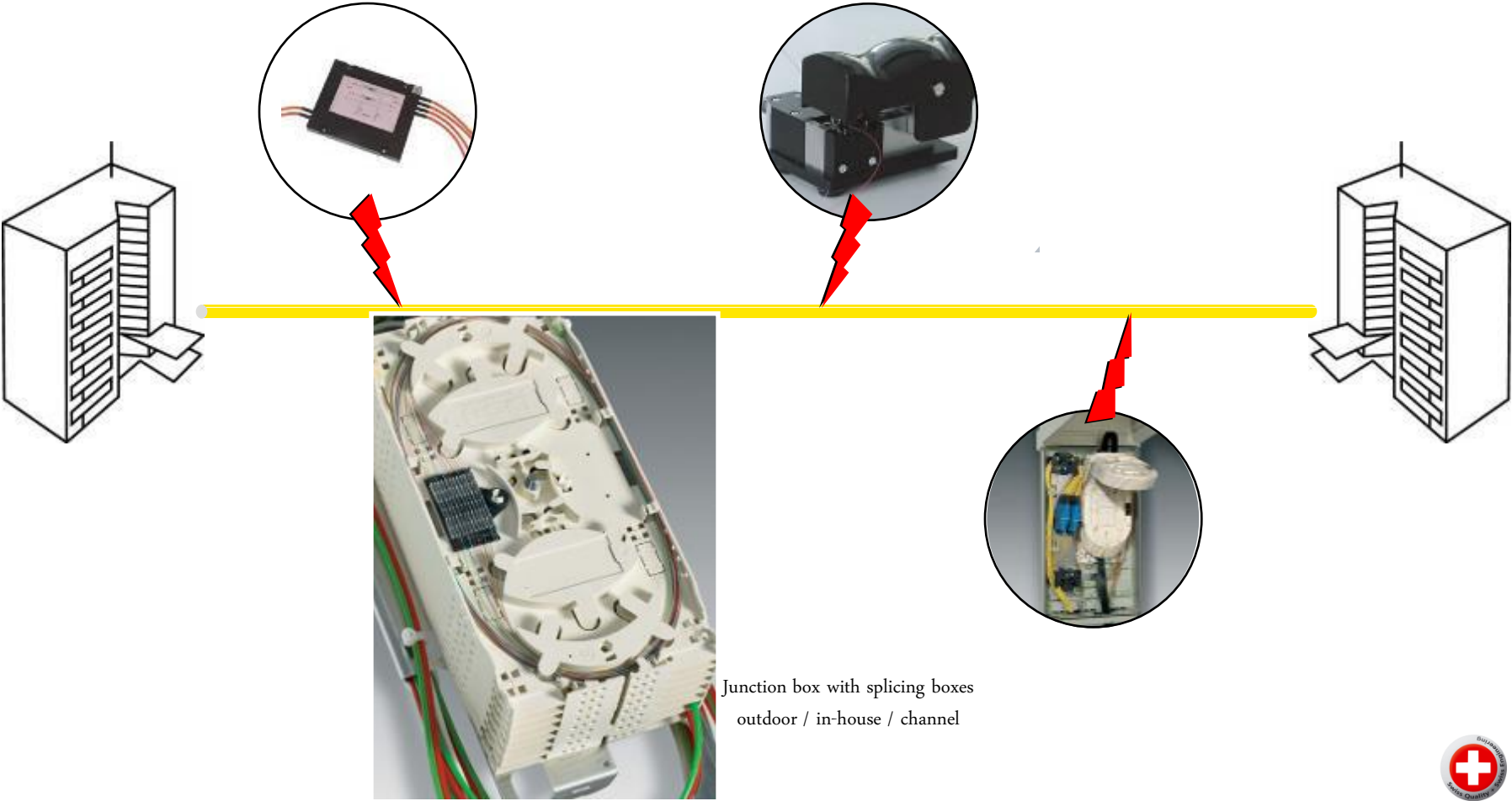
- Fibre links cannot be tapped!
- The volume of data is too large for any particular information to be targeted and read!
- Data networks using Multiplexing technology cannot be analyzed!
- Fibre Channel protocol is too complex!
- Privately owned 'Dark-Fibre' networks are inherently secure!
- Monitoring optical transmission (dB) loss across the network is sufficient!
- Encryption causes performance and latency problems!



# Fibre optics networks – tapping possibilities

Y-Bridge for service operations

Clip-on coupling device



Junction box with splicing boxes  
outdoor / in-house / channel



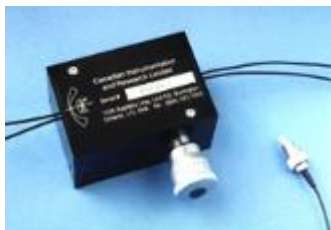
# Fibre optic networks – „optical tapping“ methods



- Splice-methods
  - This is the easiest way. A glass fibre cable is disconnected and a Y-Bridge is installed. Providers use similar devices to service their networks.



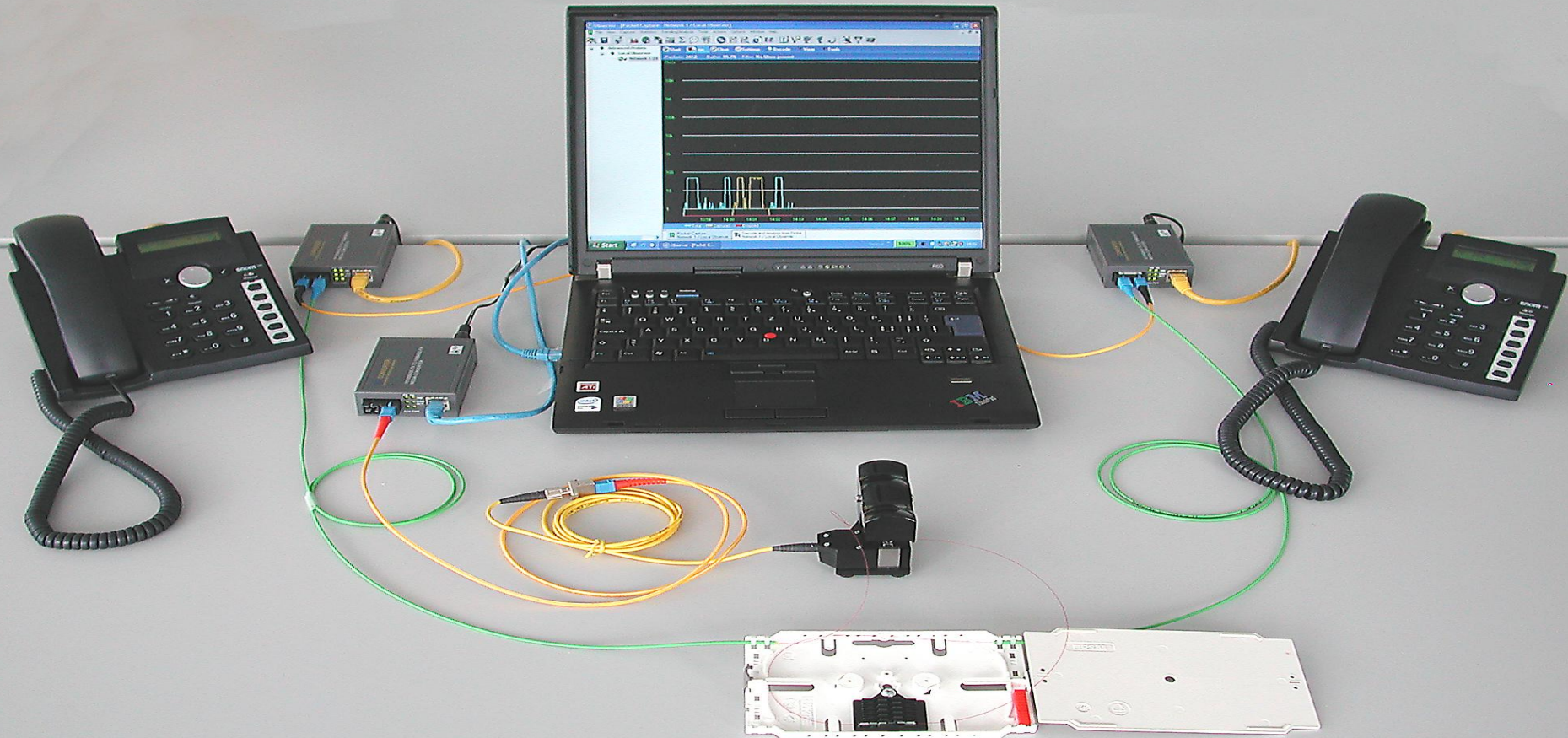
- Splitter- / Coupler-methods
  - If a glass fibre is bent, light escapes from the fibre. With today`s, modern receivers 1-2% of the optical power is sufficient to receive the complete signal and read all the data that is being transmitted.



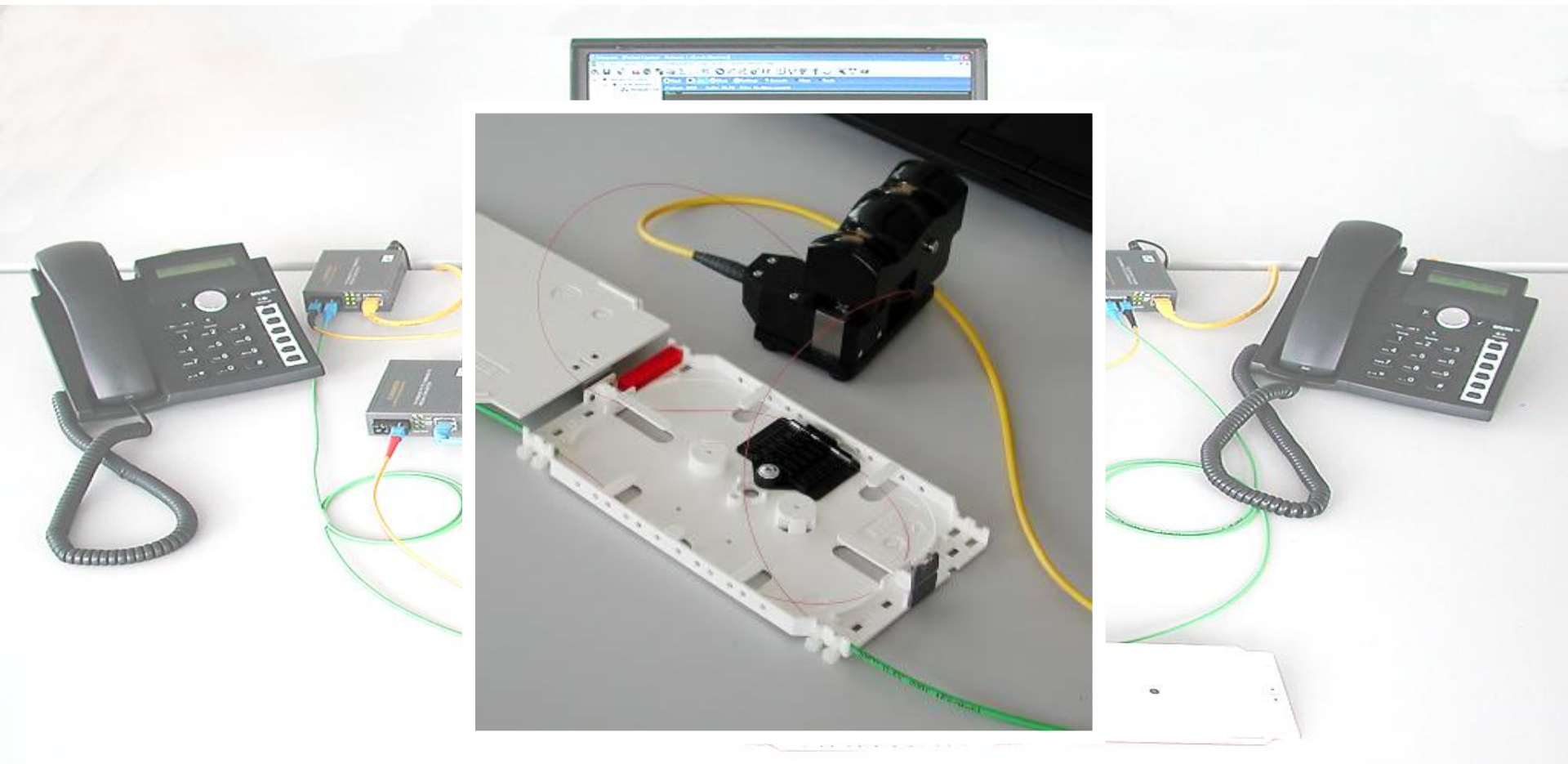
- Non-touching methods
  - Sensitive photo detectors catch a minimal amount of light which radiates naturally from the cable.



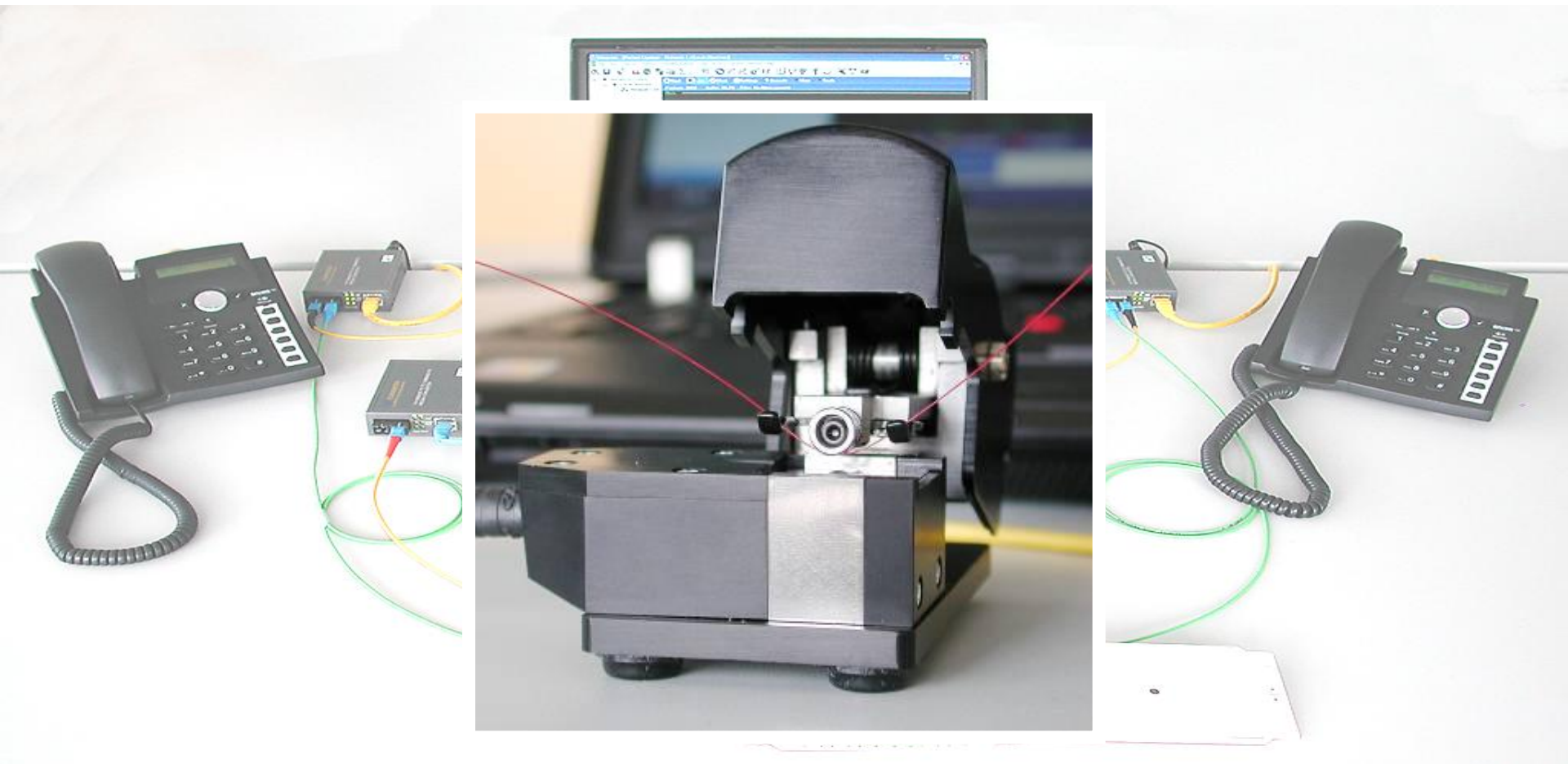
# Fibre optic networks – tapping requires little technology



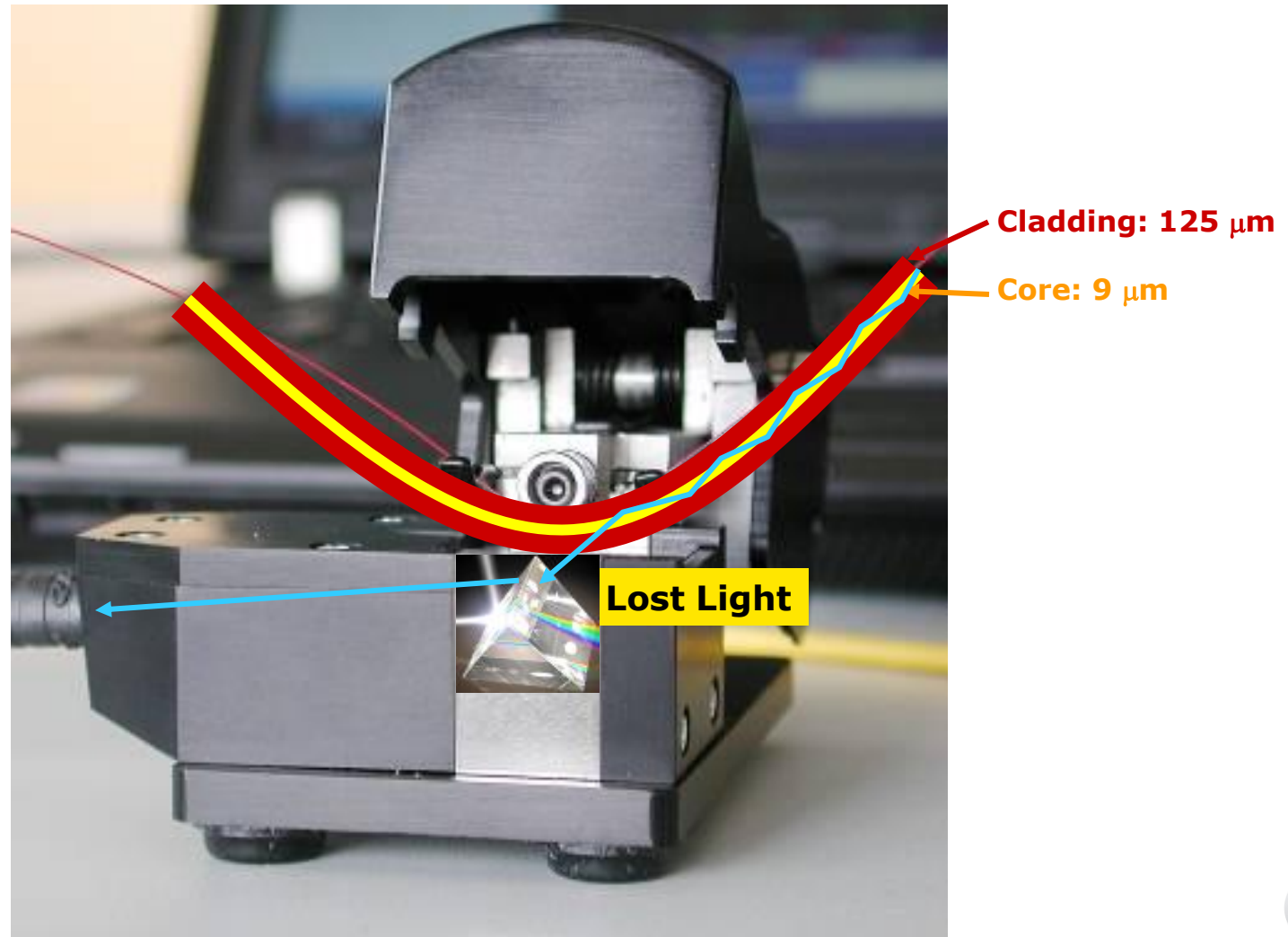
# Fibre optic networks – tapping requires little technology



# Fibre optic networks – tapping requires little technology



# Fibre optic networks – How an optical coupler functions



# Fibre optic networks – Security Myth!

## The volume or speed of data is no protection



- Hardware and software, Gigabit data analysers are freely available
- Spectrum analysers can select and filter out any particular wavelength from 1250 to 1650 nm - used in WDM technology
- Data analysers can capture and post-process all communication protocols used today: e.g. Ethernet, SONET/SDH and FC.
- Designed for network monitoring and analysis – these devices are commercially available.
- All Data traffic can easily be monitored, recorded and replayed!

Commercial splitter, coupler, splicing- and analysis tools are available for less than \$1'000 (some can be downloaded from the Internet) and absorb only up to 3dB

# Fibre optic networks – Security Myth! Fibre Channel protocol is too complex

The screenshot shows a network analysis tool interface. The top pane displays a list of events with columns for Icon, Time (mm:ss.ms\_us\_ns (R)), Port, Count - Type, Summary, Bytes, Destination, Source, LUN, and OX\_Id. The bottom pane shows a hex/ascii dump of captured data. A red box highlights a section of the dump containing a VISA card number: `##.VISA CARD. THOMAS SCHELD` followed by `..4232 5852 3660 XXXX 11/200` and `9 019. ....`.

Icon	mm:ss.ms_us_ns (R)	Port	Count - Type	Count - Type	Summary	Bytes	Destination	Source	LUN	OX_Id
FR	00:05.123_959_824	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00001800; Len = 0x800;	2084	011500	010900		00D6
FR	00:05.130_213_752	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00D6
FR	00:05.130_275_644	FC Port(1,1,1)	1 - FC4Cmd		Write(10); LUN = 0x0002; LBA = 0x005E607F; FCP_DL = 0x0	68	011500	010900	0002	00E1
FR	00:05.130_370_860	FC Port(1,1,2)		1 - FC4XRdy	DATA_RO = 0x00000000; BURST_LEN = 0x00001000;	48	010900	011500		00E1
FR	00:05.130_379_192	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000000; Len = 0x800;	2084	011500	010900		00E1
FR	00:05.130_384_228	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000800; Len = 0x800;	2084	011500	010900		00E1
FR	00:05.135_282_736	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00E1
FR	00:05.135_321_216	FC Port(1,1,1)	1 - FC4Cmd		Write(10); LUN = 0x0002; LBA = 0x005E606F; FCP_DL = 0x0	68	011500	010900	0002	00F3
FR	00:05.135_410_364	FC Port(1,1,2)		1 - FC4XRdy	DATA_RO = 0x00000000; BURST_LEN = 0x00001000;	48	010900	011500		00F3
FR	00:05.135_416_932	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000000; Len = 0x800;	2084	011500	010900		00F3
FR	00:05.135_423_968	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000800; Len = 0x800;	2084	011500	010900		00F3
FR	00:05.139_213_964	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00F3

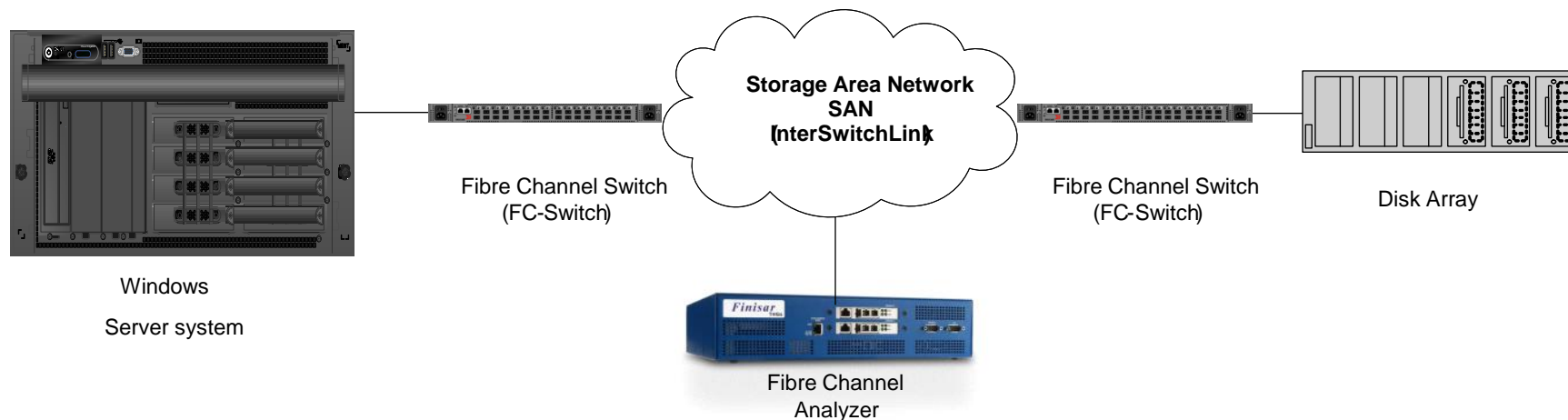
  

Index	Hex	Ascii
04D0	00 00 00 00 1B 00 01 00 28 00 00 00 28 00 04 00 18 00 00 00 00 00 00 00 00 00 00 00	.....P.t.N.....eT.....
04EC	00 00 00 00 00 00 00 00 50 15 74 D1 03 00 00 00 9C 54 00 01 00 00 00 00 00 00 00 00	.....H.....
0508	00 00 00 00 00 00 00 00 07 00 07 00 28 00 85 00 B8 00 85 00 18 00 01 00 20 01 18 00	.....t.....s.....
0524	00 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 23 23 23 23 23 23 23 23	.....#####
0540	04 00 00 00 07 00 00 00 00 00 00 00 07 00 0C 00 00 00 00 00 23 23 23 23 23 23 23 23	.....#####
055C	23 23	.....#####
0578	23 23 0D 0A 56 49 53 41 20 43 41 52 44 0D 0A 54 48 4F 4D 41 53 20 53 43 48 45 4C 44	##.VISA CARD. THOMAS SCHELD
0594	0D 0A 34 32 33 32 20 35 38 35 32 20 33 36 36 30 20 58 58 58 58 58 20 31 31 2F 32 30 30	..4232 5852 3660 XXXX 11/200
05B0	39 20 30 31 39 0D 0A 23	9 019. ....
05CC	23 23	.....
05E8	00 00	.....
0604	00 01 00 00 00 00	.....

Source: Brocade Communications Systems, Inc.



# Fibre optic networks – Security Myth! Fibre Channel protocol is too complex



Simply mirroring data!

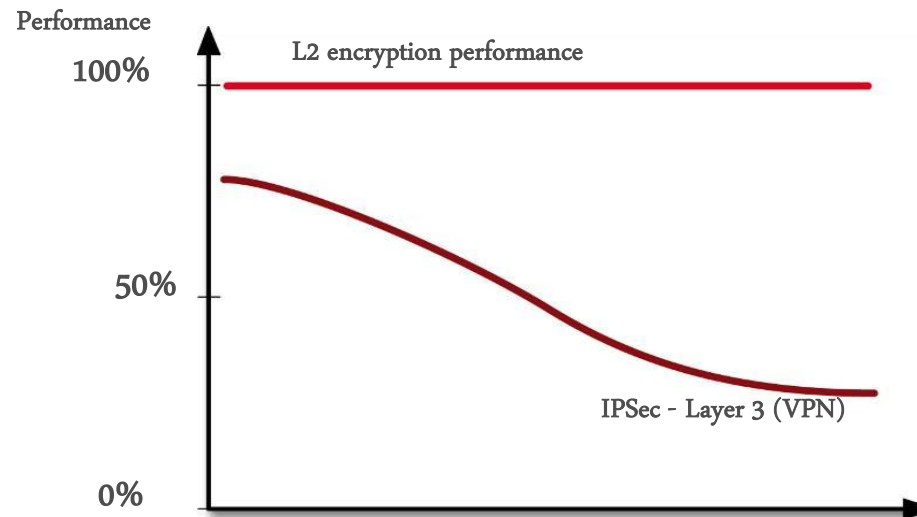
- **FC-analyzer records data traffic**; includes: all SCSI-commands, Logical Block Addresses, and read – write Commands – *information now readable in this format*
- **Export from FC-analyzer** – to a CSV-file and convert into a binary file by means of a simple Unix script
- **Create a mirrored copy** Mount binary file using “ImDisk” in Windows-Explorer, recorded data appears as an additional disk in Windows-Explorer

# Fibre optic networks – Security Myth! Encryption causes latency problems



## ■ Performance

- IPSec (Layer 3) creates considerable overhead (+ 57 Bytes) and massively reducing the actual useful data rate.
- InfoGuard Layer 2 encryption



(e.g. 64 Bytes Packet = 47% of the whole Traffic is overhead)

- 65% of the worldwide IP-Traffic are small IP-Packets. (64 Bytes and 128 Bytes)



# Fibre optic networks – Security Myth

## How can confidentiality really be guaranteed?



Myth Loch Ness

- Fibre links cannot be tapped
  - **Fibre links can be monitored!**
- The volume of data is too large and Multiplexing technology cannot be analyzed
  - **An illusion!**
- Fibre Channel protocol is too complex
  - **Data analyses are commercially available!**
- Privately owned 'Dark-Fibre' networks are inherently secure
  - **Insufficient protection!**
- Monitoring optical transmission (dB) loss across the network is sufficient
  - **A good first start but not enough – monitoring devices get more sophisticated**
- Encryption causes performance and latency problems
  - **Layer 2 encryption guarantees 100% performance and minimal latency!**

There's only one secure and economical way to guarantee confidentiality:  
**Layer 2 Encryption**





- Maximal performance
  - 100% encryption of 1Gbps up to 10 Gbps
  - Maintains a constant low latency
    - Ethernet 1G: < 3 $\mu$ s
    - Ethernet 10G: < 1 $\mu$ s
    - SONET/SDH 10G: < 1 $\mu$ s
    - FC 1/2/4G: < 40 $\mu$ s
    - EGM (20/100M): < 150 $\mu$ s
    - EGM1 (200M/1G): < 30 $\mu$ s



- High flexibility seamless integration
- Strong data encryption
- Easy administration
- High availability
- Swiss product



# InfoGuard Network Encryption – encryption solution for each requirement!

## Ethernet

### Point-to-Point



- 1 / 10 Gigabit Ethernet Data Encryption
- Layer 2 Solution
- Usable for high performance connections over Dark Fibre, DWDM, CWDM and SAN-Extension

### Point-to-Point Multipoint-Multipoint



- 20 / 100/ 200 Mbps and 1Gbps Ethernet Data Encryption
- Layer 2 Solution
- Usable in Point-to-Point and Multipoint Ethernet Networks (EPL, EVPL, EPLAN, and EVPLAN)

## SONET/SDH

### Point-to-Point



- OC-192 / STM-64 and OC-12 / STM-4\* SONET/SDH Data Encryption
- Supports Path- and Line-Encryption
- Flexible and cost effective combination of different services with TDM cards

\* available Q1/2009

## Multilink Multiprotocol

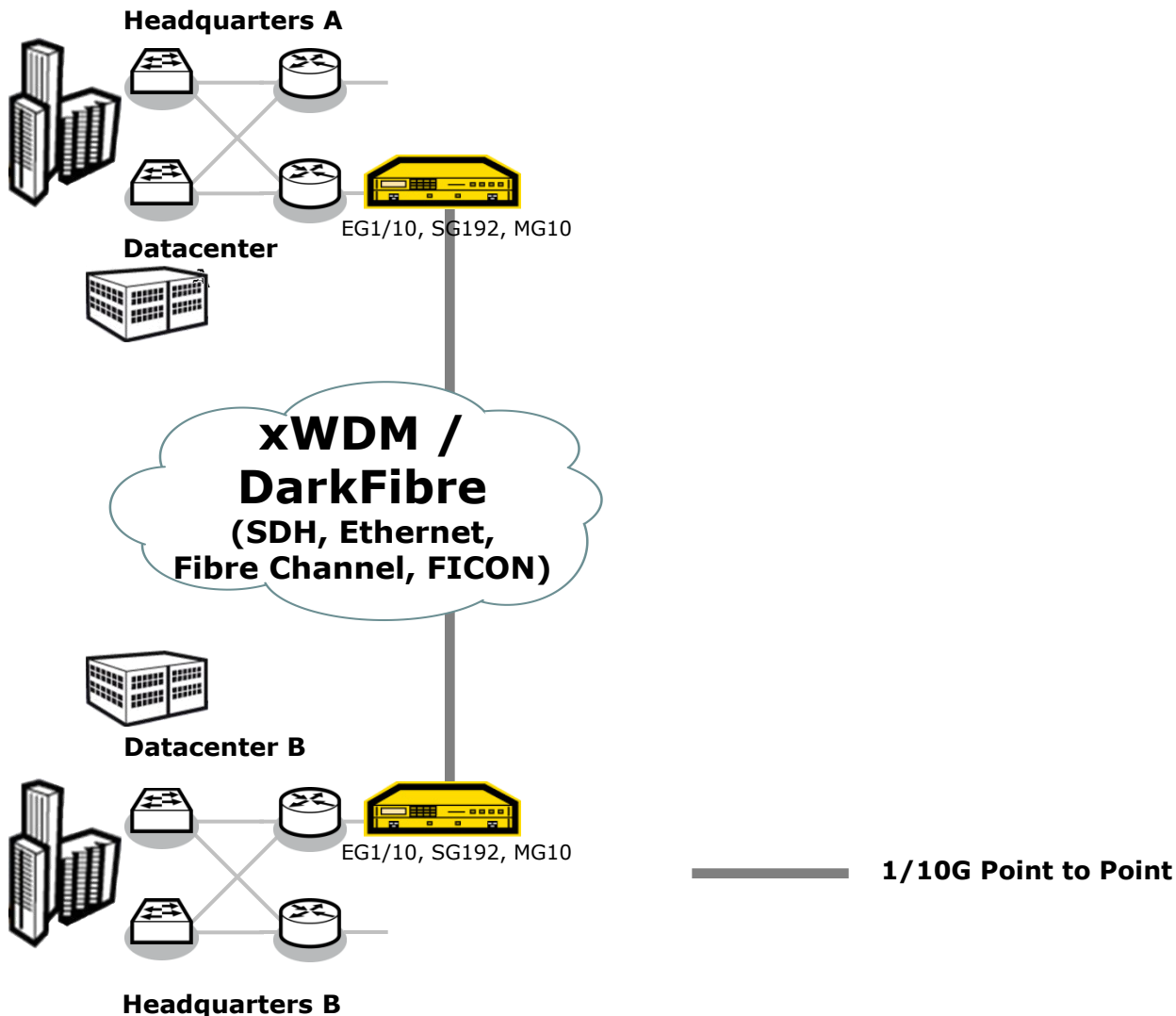
### Point-to-Point



- GbE, Fibre Channel and FICON Data Encryption up to 10Gbps
- Mapping and encryption of up to 10 channels into a single link



# InfoGuard Network Encryption – Typical L2 Point-to-Point Encryption Scenario





infoGuard

and information becomes secure

ADVA™  
Optical Networking



## InfoGuard Network Encryption

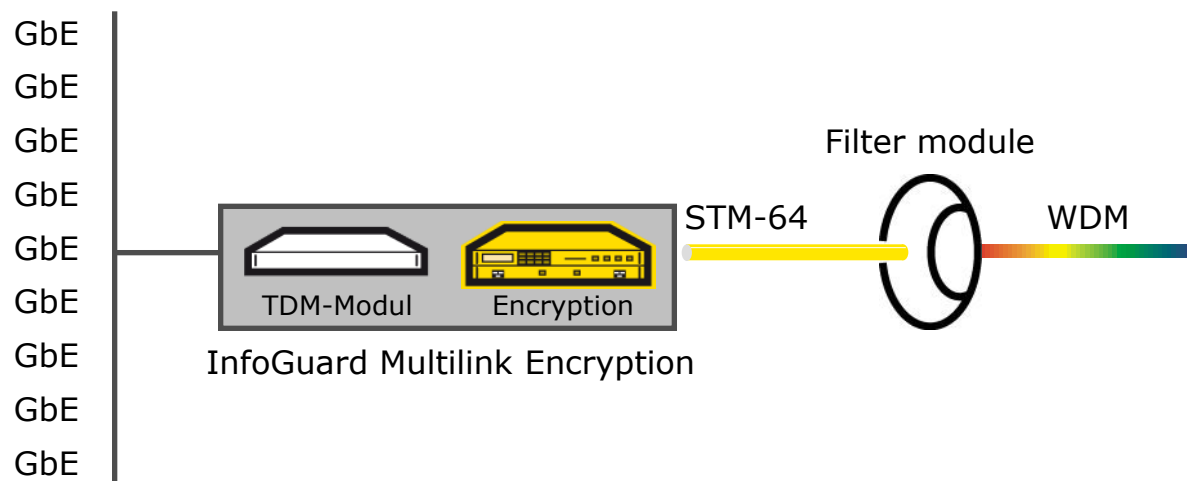
Multilink / Multiprotocol Encryption –  
Flexible and Cost Efficient Data Encryption for Ethernet,  
Fiber Channel and FICON.



# Multilink / Multiprotocol Encryption – application scenario

Mapping of up to 9 Ethernet channel into a single link.

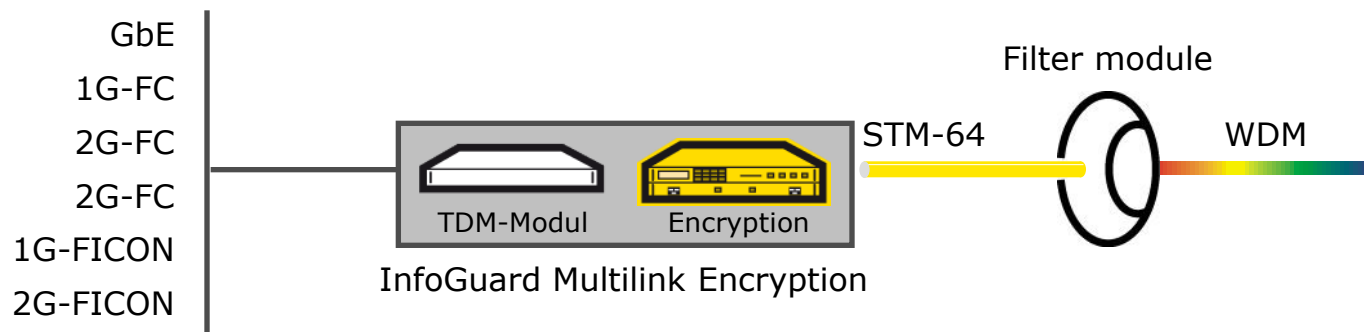
- Client side: 9xGbE
- Network side: Encrypted OC-192/STM-64 frame



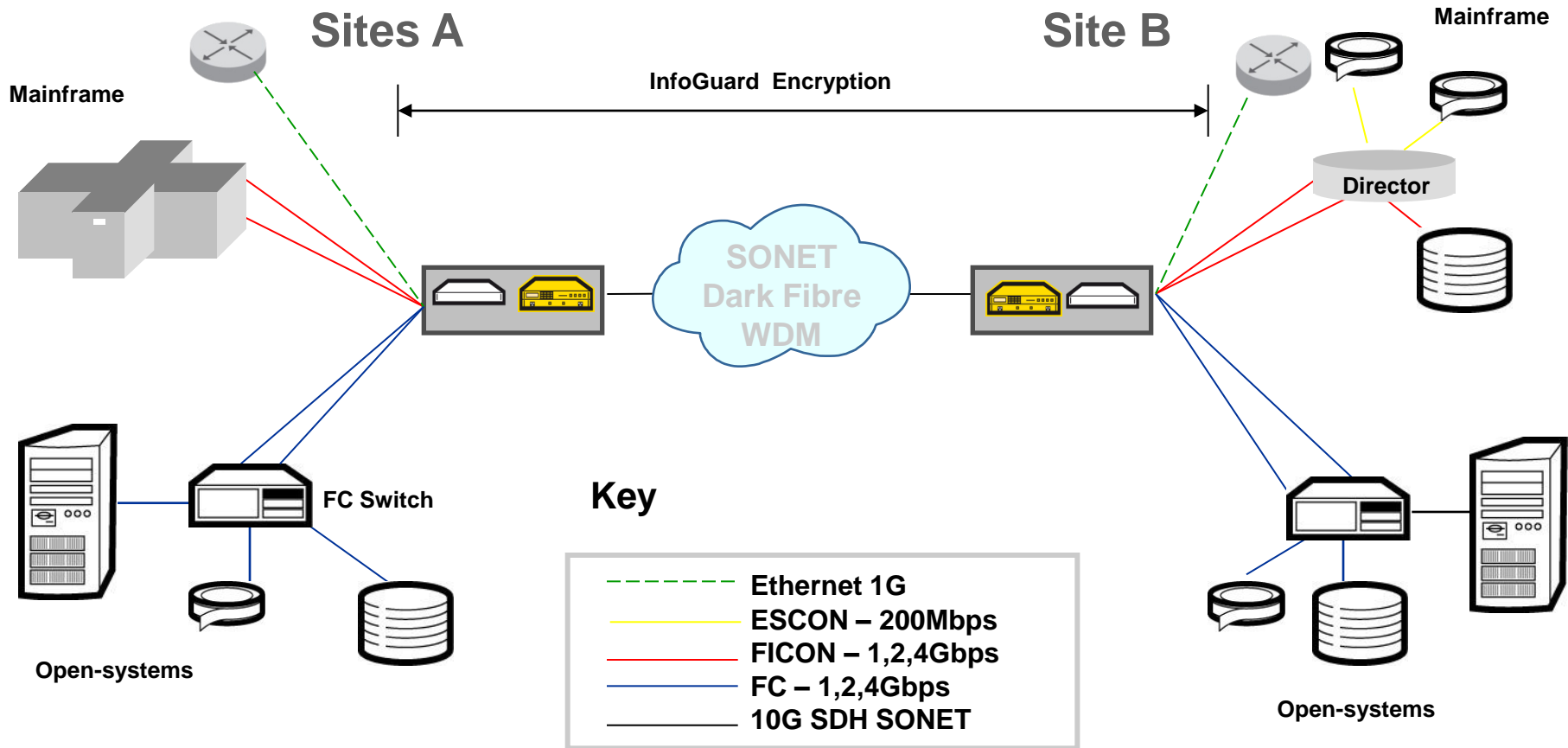
# Multilink / Multiprotocol Encryption – Protocol multiplexing application scenario

Mapping of heterogeneous LAN/SAN signals  
(Ethernet, Fibre Channel, FICON) into a single link.

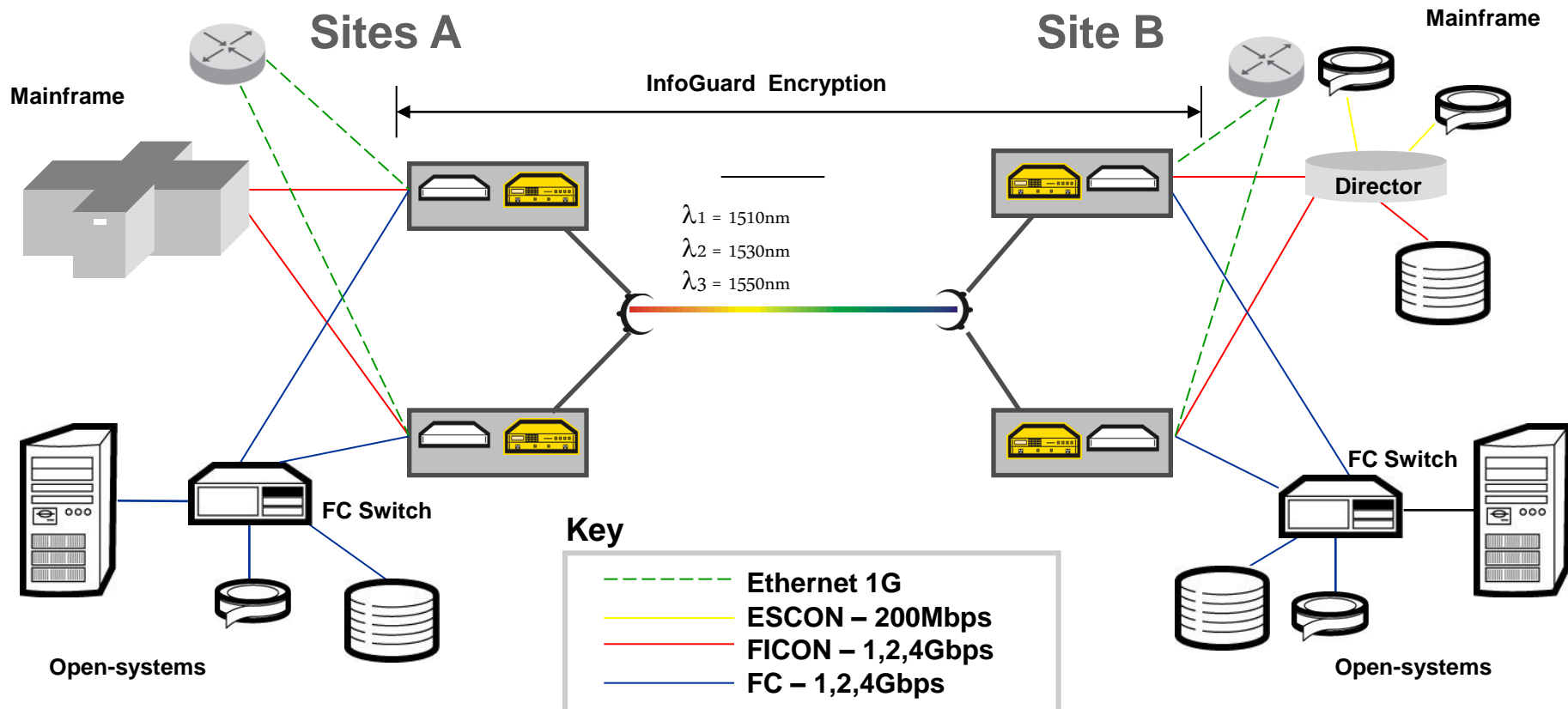
- Client side: 9xGbE, 10x1G-FC, 10x1G-FICON, 5x2G-FC, 5x2G-FICON, 2x4G-FC
- Network side: Encrypted OC-192/STM-64 frame



# Customer example: Encrypting SAN's over SONET, WDM or Dark Fibre



# Customer example: Encrypting SAN's over CWDM networks



# Encryption of Information as a «Best Practice» – References

- Provided enterprise Encryption Solutions for high-speed Networks since 2003
- 'Best Practice' in Swiss Banks
- More than 1'000 devices installed around the world provides sound proof of product and company reliability
- Several European Central Banks
- Various government organizations around the world



- With today's professional hackers, cyber crime is clearly on the increase.
- If core backbone networks are not protected the consequences of a breach could be devastating and immeasurable
- Governments and regulatory institutions are placing increasing pressure on organisations to adequately protect our data.
- Today's encryption capability provides a seamless and cost effective method to secure SAN's in MAN and WAN environments
- Are you sending confidential information across unprotected networks?



# InfoGuard worldwide Partner Network



## Strategic Partnerships



## Distribution Partner



## Reseller

Germany



England



Poland



Scandinavia



Estonia



Netherland



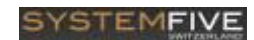
Italy



France



Switzerland



Canada

