Fraud Overview

TAF Regional Seminar on Costs and Tariffs, 28-31 January 2008, Djibouti

Peter Hoath

peter.hoath@bt.com

Agenda

- Fraud introduction and overview
- “Standard” fraud types
- Some more recent fraud types
- The next generation of fraud
- Countermeasures

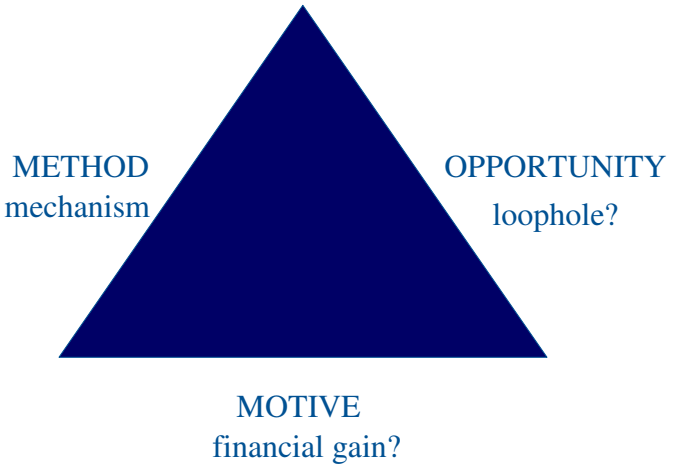
The cost of fraud to the industry

- $30 Billion per annum?
- $50 Billion per annum?
- Estimates vary but probably stable around this figure worldwide for the past 5 years
- A value of up to 6% of total company revenue is not unusual
- Control to less than 1% of total revenue is regarded as a good performance

A fraud definition for the industry

- The use of the telecommunications network with the intention of avoiding payment.
  - without correct payment
  - with no payment at all
  - someone else pays.

The Fraud/Crime triangle

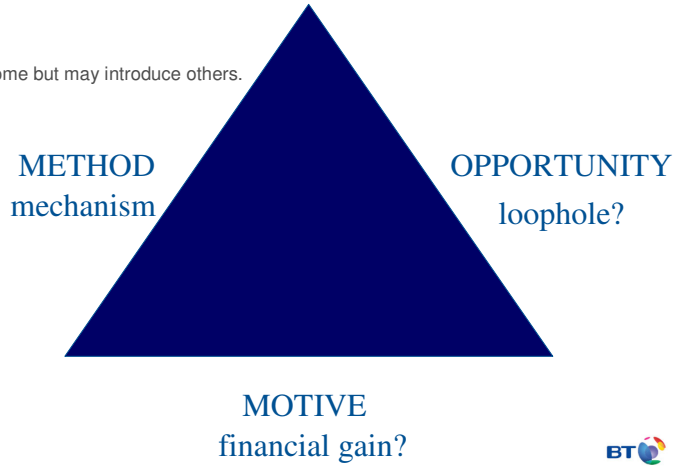


Characteristics of telecommunications fraud

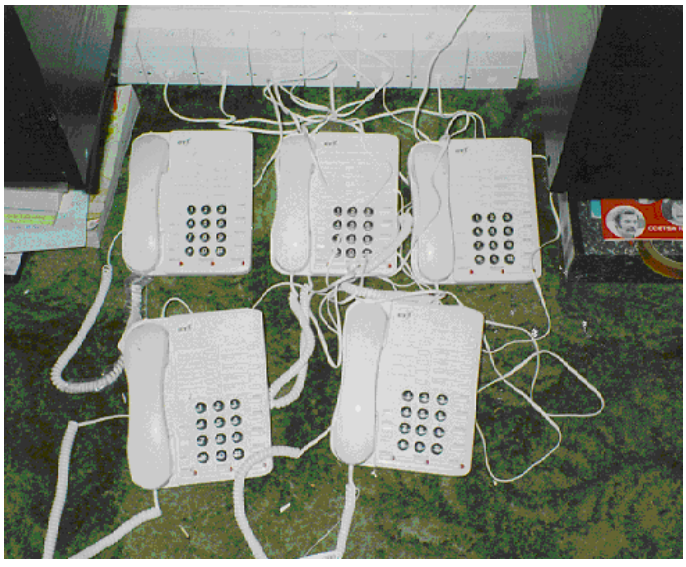
- Telco fraud seen as victimless
- Crime committed remotely minimises detection risk
- Often, no equipment is needed - knowledge rather than a crow-bar
- Easy conversion to cash - eg call selling
- Products are complex and lend themselves to interactions.

Solutions overview

- Remove the motive
  - hard to do if tariffs are high
- Deny the opportunity
  - physical security?
- Fix the method
  - new technologies fix some but may introduce others.



"Standard" frauds – Call Selling



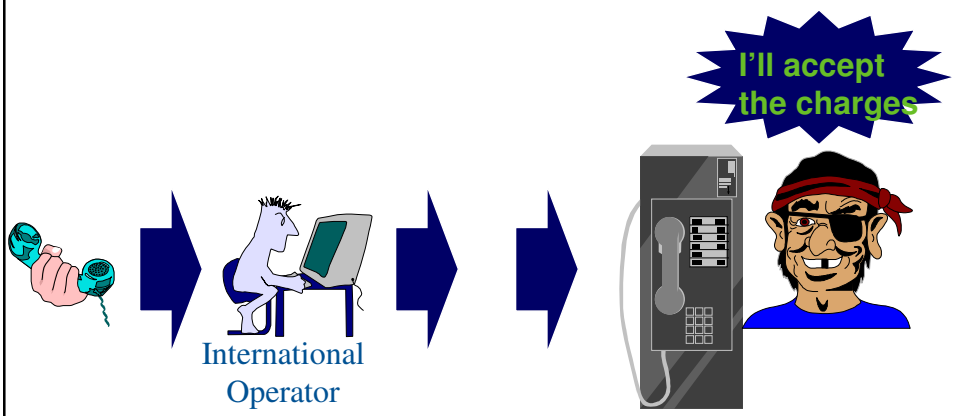
“Standard” frauds – Call Selling

- No intention to pay – so this is also **Subscription Fraud**
- When used in conjunction with call diversion the “customer” does not need to be present
- Detection is relatively easy using modern billing systems
- Consider how to vet customers applying for service. Why would he want 7 telephones in one apartment?

“Standard” frauds – Payphones

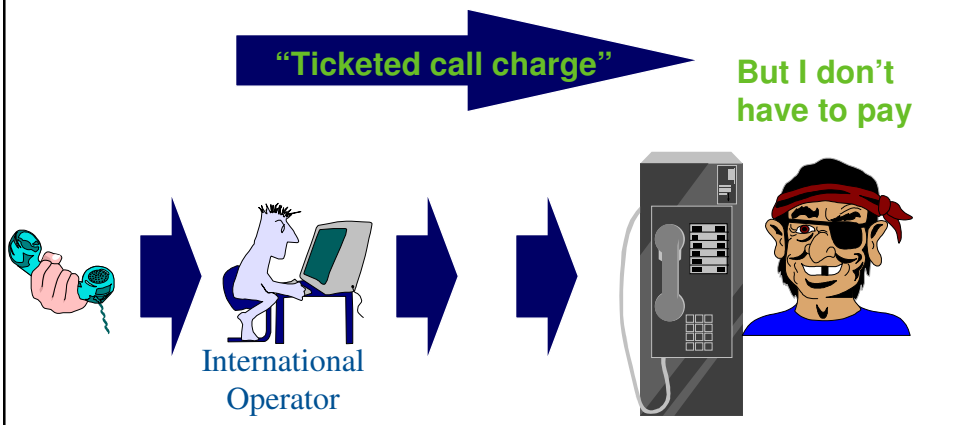
- Payphone software bugs have been a problem
- Cash payphones may suffer physical abuse
- Pre-payment or credit card payphones can reduce fraud
- Collect calling to payphones has been a problem…

"Standard" frauds – Payphones



COUNTRY A COUNTRY B

"Standard" frauds – Payphones



COUNTRY A

COUNTRY B
telco is the loser

“Standard” frauds – Payphones

Countermeasures

- do not allow incoming calls to payphones
  - may not be permitted under regulatory system
- “cuckoo” tone on incoming calls to payphones
  - can be defeated by shouting
- SS7 countermeasures
  - discriminates by detecting PCO in SS7 ACM message
  - passes the call to a local operator for connection.

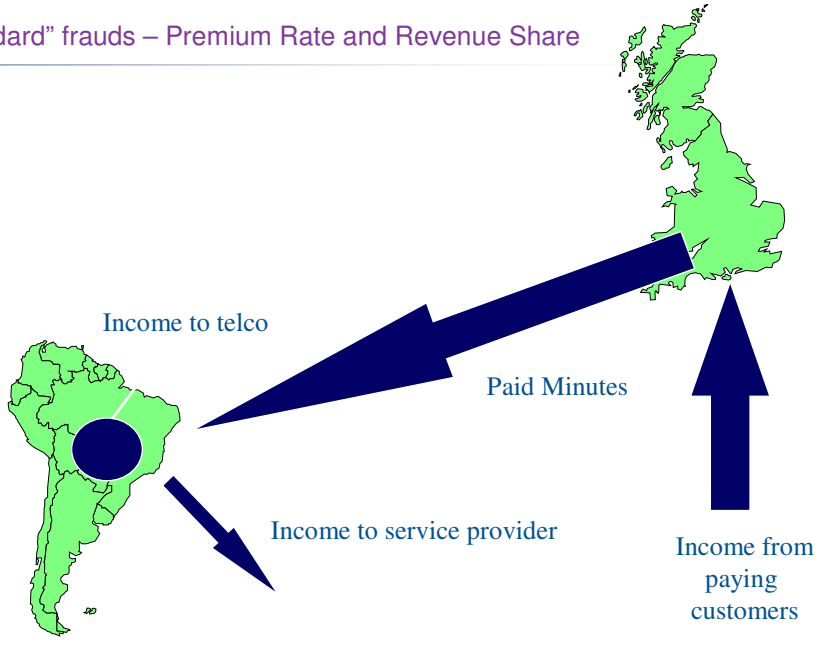
“Standard” frauds – Subscription Fraud

- Be aware of the distinction between “Cannot pay” and “No intention to pay”
- Probably the most widespread fraud type globally
- Also extends into the Mobile market place
  - Multiple fraudulent applications for service
  - Handsets sold - possibly abroad
    - if bought in a country where heavily discounted and sold in a country where full price is levied....arbitrage
  - SIM cards shipped abroad and heavily used
    - maybe part of call selling scam.

“Standard” frauds – Premium Rate and Revenue Share

- Sometimes called Audiotext services
- In country PRS/Revenue share services usually in a separate number range.
- High tariffs for the customer
- The terminating number receives a share of the billed revenue, around 50% is typical.
- It gets very complex when interconnection between carriers is involved. Cooperaton is key.
- The fraudster’s goal is to inflate traffic to his PRS or Revenue Share numbers at little or no cost to himself
  - Therefore subscription fraud, fixed and mobile, will also be used to commit PRS fraud
- Some PRS operators have engaged with international telcos to provide this type of service
- We have seen hijacking of whole number ranges by unscrupulous Revenue Share operators
- Sometimes these calls have been short-stopped and terminated in a different country

“Standard” frauds – Premium Rate and Revenue Share



"Standard" frauds – Premium Rate and Revenue Share

- We have seen many different ways to inflate calling rates
  - Spam – call this number
  - Clip on or tee-ing in to customer lines
  - Autodiallers
    - Personal Computer based
    - Built in to customer line jack
  - Pyramid Selling
  - Pager messages – call this number
  - Internet Diallers
- This practice is called "Artificial Inflation of Traffic"
  - If detected it is possible to withhold onward payment for the traffic – by negotiation with the in-country Regulator. This is done in the UK.
- Some PRS/Revenue Share numbers are charged to the caller on a so called "Single Drop", or "Flag Drop" basis irrespective of call duration. This leads to
  - Frauds involving very short calls, either to generate very large amounts of traffic as part of a subscription fraud, or to defeat the billing system at the originating point.

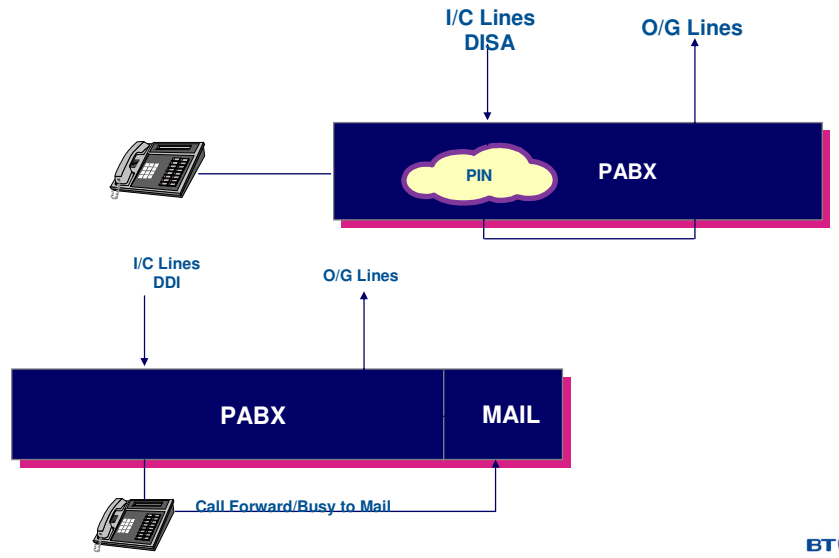
BT

"Standard" frauds – PBX Dial Through Fraud

- Major phenomenon late 1980s to date
- Major business success (for the bad guys)
- Involves illegal reprogramming or abuse of a PBX and its facilities to route calls at reduced or nil cost to the caller
- Motivation:
  - To avoid detection by call tracing:
  - Free phone calls – personal or call-selling
  - To facilitate computer hacking
  - In conjunction with other scams - PRS fraud
  - Substitute for other "closed" methods

BT

“Standard” frauds – PBX Dial Through Fraud



“Standard” frauds – PBX Dial Through Fraud Countermeasures

Users

- Education
- Process improvement
- Awareness
- Usage records
- Configuration

Vendors

- Good design
- Advisories
- Upgrades
- Customer relations
- Information disclosure

Telco

- Network monitoring
- Notification
- Education
- Customer relations
- Insurance

More Recent – Arbitrage or Rate Fraud

- Exploitation of:
  - differing accounting rates,
  - complexity of services and rates,
  - multi-operator environment.
- Service Provider makes deal with Telco B. Telco B charges Telco A at wholesale rate for call termination. IF Telco A does not recognise that the call is at a higher tariff then it will not recover..
- In some cases not fraud, not illegal, current target for unscrupulous Service Providers and possibly criminals.
- We have seen tromboning of calls across international borders
- Wimax offers new possibilities with its 50km range
- Telcos withhold outpayments to Service Providers or Telcos if Artificial Inflation of Traffic is suspected/proven
- Detection via traffic level deviation, call durations, origination points, fraudulent methods
- International rates offered to customers by some startup companies seem impossibly low – suspicion that someone is losing out
- Vital area for Telcos to exercise vigilance

BT

More Recent – International Bypass

- Motivated by high terminating rates to some countries
- New technologies are providing the means to extend services across international borders – eg WiMax.
  - The principle is not new, GSM service has extended across borders for some time but this has usually been accidental and not by design.
- Internet delivery using Voice over IP is a new development, for example in conjunction with GSM Gateway (SIM box).
- Services like Skype are putting pressure on telcos to reduce tariffs.
- Local legislation and Regulatory regime varies – sometimes illegal, sometimes not.
- Some tariffs advertised, for example in the UK, are amazingly cheap. How are these calls routed???

BT

More Recent – International Resale

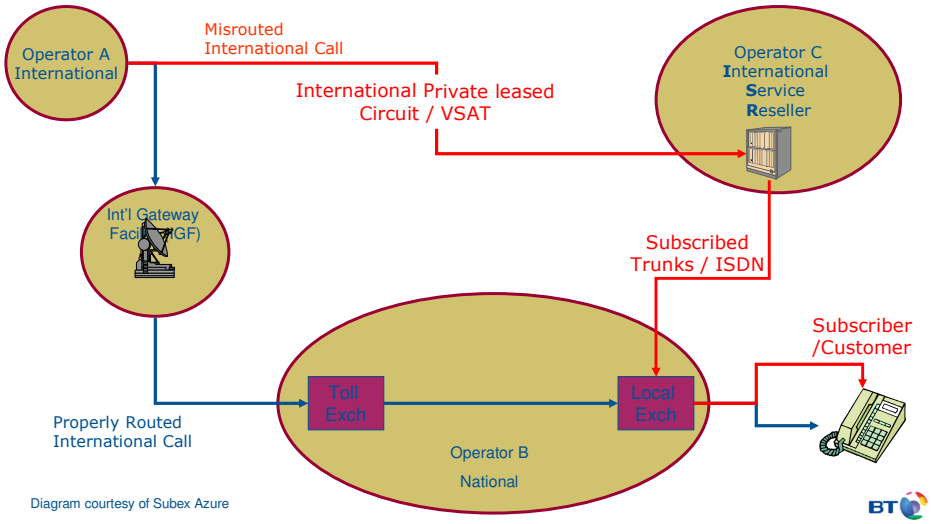


Diagram courtesy of Subex Azure

BT

More Recent – VoIP bypass

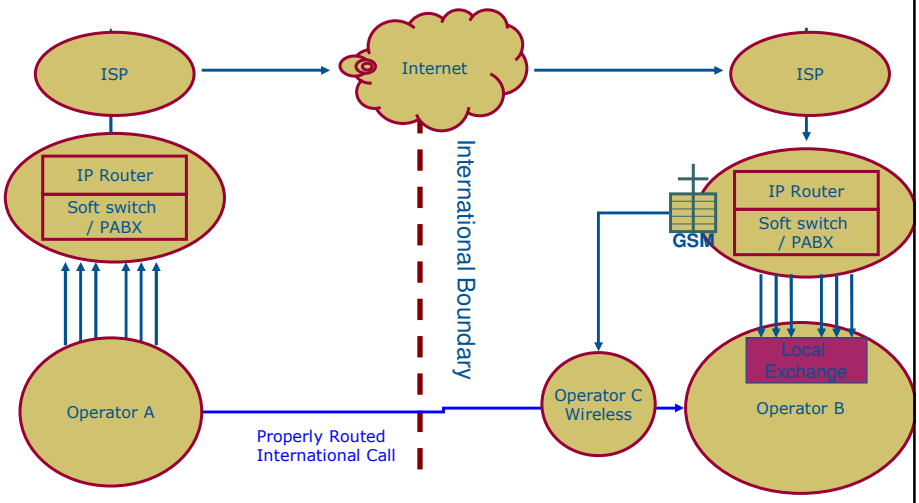


Diagram courtesy of Subex Azure

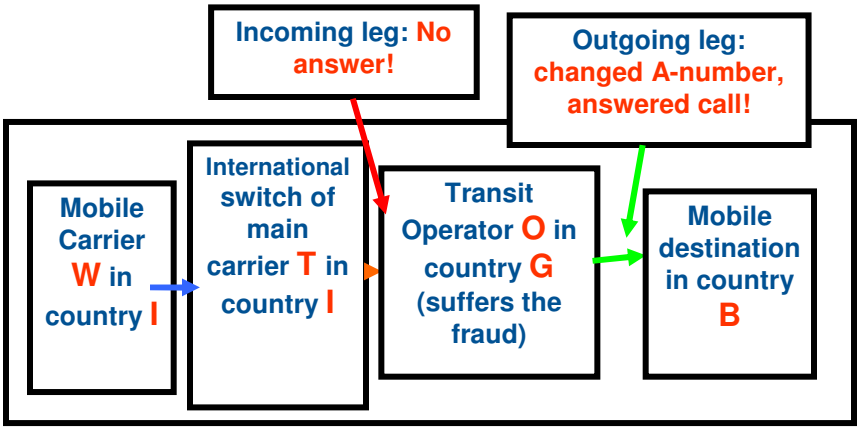
BT

More Recent – Inter-carrier fraud, a worrying development

- Manipulation of Signalling System #7 Calling Party Category
- A switch manufacturer decides to load standard software onto all switches, national and gateway.
- Then the switch manufacturer released a patch to allow Voicemail interrogation by using a special CPC (non-ITU) and a special non-existent A-number. This patch was installed in **Country G**.
- Subsequently, **mobile operator W** in **Country I** falsely used this new CPC to send mobile calls via **Country G** for onward termination. Calls recognised as voicemail, not normal traffic. Therefore no answer signal returned to **Country I** but **Country G** is charged for the onward call and loses because they collect no revenue for handling the call.

BT

The scenario



BT

Next Generation Fraud

- WiFi resale
- “Click Fraud”, a form of content provision fraud
- Denial of service attacks
- Botnets
- As networks become homogeneous and IP based, the world of telecommunications fraud will become part of an overall Cyber Crime picture.

Cybercrime

- A computer or network may be a tool of the criminal activity include spamming and criminal copyright crimes, particularly those facilitated through peer-to-peer networks.
- A computer or network may be a target of criminal activity include unauthorized access (i.e, defeating access controls), malicious code, and denial-of-service attacks.
- A computer or network may become a place of criminal activity include theft of service (in particular, telecom fraud) and certain financial frauds.
- Finally, traditional crimes may be facilitated through the use of computers or networks include Nigerian 419 or other gullibility or social engineering frauds (e.g., hacking "phishing", identity theft, child pornography, online gambling, securities fraud, etc. Cyberstalking is an example of a traditional crime -- harassment -- that has taken a new form when facilitated through computer networks.
- Additionally, certain other information crimes, including trade secret theft and industrial or economic espionage, are sometimes considered Cyber Crimes when computers or networks are involved.
- Cyber Crime in the context of national security may involve hacktivism (online activity intended to influence policy), traditional espionage, or information warfare and related activities.

Cyber criminals may be

- Hackers, Malicious insiders
- Industrial espionage
- Bored, disgruntled, or overburdened employees
- Naive/uninformed computer users
- Organized crime
- Terrorists
- Pedophiles and molesters

Cyber crime dividends

- Hackers teamed with professional criminal gangs in increasingly sophisticated computer crime operations aimed purely for profit.
- Law enforcement agencies are getting more organized and cooperating better, particularly in international investigations. At least 45 countries participate in the G8 24/7 High Tech Crime Network, which requires nations to have a contact available 24 hours a day to aid in quickly securing electronic evidence for trans-border Cyber Crime investigations.
- The private sector has also helped. Microsoft filed dozens of civil suits and gave information to law enforcement for criminal cases in Europe, the Middle East and the United States against alleged phishers throughout 2006 and 2007.

Cyber crime in Africa

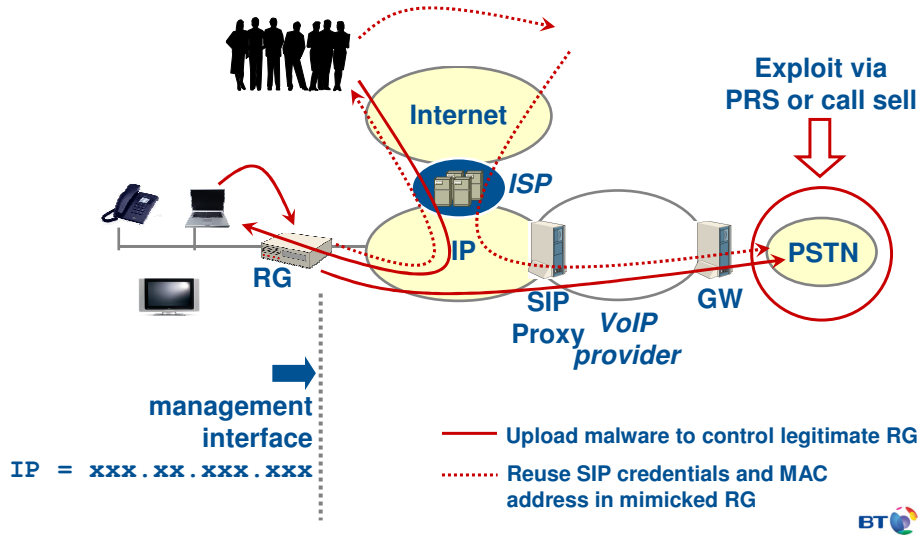
- Current research indicates Africa is not the source or the target of major cyber attacks, but
  - Africa is still very vulnerable to most major attacks.
- The evolution of Cyber Crime (active to passive)
  - Could negate any protection limited connectivity may have provided in the past.
- Impact of increased capacity with insufficient security technology, expertise and policies:
  - Africa as an entry point for cyber criminals and terrorist using it as a hub to coordinate and launch attacks.

Merging what we have seen together – for 2007/2008

- Wholesale Fraud, carrier to carrier
- Fraud with calling card
- SMS Fraud & Security
- SS7 vulnerability – (Hyper-short calls and Voting TV) - a revenue share fraud
- Critical Infrastructure Protection – Botnets
- Threats on E-commerce (including credit card fraud)
- VoIP Fraud & Security + IP PBX HACKING
- Pharming + Phishing
- International Resale Fraud and roaming fraud
- Dialers (Decreasing due to ADSL implementation)
- Click fraud. In average 10% of all ad clicks are invalid (advertisers to pay an extra $16 billion a year).
- Cable theft – the cancer eating at the heart of the fixed network
  - Copper Cable Theft is a worldwide problem

Coming soon for some and here already for others

New Technology – Residential Gateway Abuse
Scenarios



What does this mean for the incumbent?

- More actors
  - SS7 Telecom network were secure because of limited access
  - Now small companies get SS7 network elements just for billing (think 'new entry points')
- Need for more flexibility
  - IP based networks enable fast setup, well known
  - Use of open tools & stds, faster development
- Result:
  SS7 world and IP world are colliding!
  New protocols appear (SIGTRAN)

Countermeasures

- Invest in a fraud management system. FMS vendors are eager to engage.
- Invest in network monitoring tools and the skills to use them
- Simple (and inexpensive) control measures can eliminate up to 80% of fraud exposure
  - Billing system threshold checks
  - Customer credit vetting
  - Customer deposit schemes
- Help is available – eg FIINA, SATA, AICEP, CFCA
  - **Forum for International Irregular Network Access – FIINA**
  - Free membership for telcos with international service (RPOA)
  - Annual plenary meetings, conference calls throughout the year
  - Expert advice and cooperation between telcos
  - Someone in FIINA will very likely have the answer to your problem
  - Membership enquiries to Peter Coulter of AT&T, peter.coulter@att.com

BT

Thank you

BT