

Cyber Crime and Critical Information Infrastructure impact

Luis S Cardoso
FIINA President
Portugal Telecom
LuisSCardoso@ieee.org



Cyber Crime has outstripped illegal drug sales worldwide, and analysts estimate online fraud will bring in \$105 billion in 2007.

The continued vulnerability of online information and financial access points is an enormous concern for many industries, police agencies and the military, and the sophistication of the thieves grows each year, as well.

(InformationWeek 500 conference, Tucson)

The FBI in a McAfee study estimates the total cost at over \$400 billion

Cyber Crime

Cyber Crime is a term used broadly to describe activity in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories.

- **Examples of Cyber Crime in which the computer or network is a tool of the criminal activity include spamming and criminal copyright crimes, particularly those facilitated through peer-to-peer networks.**
- **Examples of Cyber Crime in which the computer or network is a target of criminal activity include unauthorized access (i.e, defeating access controls), malicious code, and denial-of-service attacks.**
- **Examples of Cyber Crime in which the computer or network is a place of criminal activity include theft of service (in particular, telecom fraud) and certain financial frauds.**
- **Finally, examples of traditional crimes 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.**

Who are Cyber Criminals?

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

Cyber Crime

- **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.**

The Origins

Telecommunications security problems started in the 1960's when the hackers of the time started to discover ways to abuse the telephone company.

BUT...how they do?

- **Discovery and exploration of features of telecommunications systems**
- **Controlling Network Elements (NE) in a way that was not planned by its designers**
- **Abusing weaknesses of protocols, systems and applications in telephone networks**

NETWORKS and PAYLOAD

Networks



Payload

The various topological

- configurations of nodes
- synchronization
- redundancy
- physical and logical diversity
- network interconnections
- availability
- operations

Transported Content on network

- Signaling
- Voice
- Data
- Multimedia

Payload Security

- Information interception
- Information corruption

Traffic patterns and statistics

INTRINSIC VULNERABILITIES

Networks



Payload

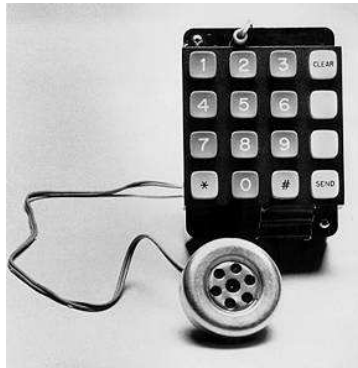
VULNERABILITY

capacity limits
points or modes of failure
points of concentration (congestion)
complexity
dependence on synchronization
interconnection (interoperability, interdependence, conflict)
uniqueness of mated pairs
need for upgrades and new technology
automated control (*via software)
accessibility (air, space or metallic or fiber)
border crossing exposures

VULNERABILITY

unpredictable variation
extremes in load
corruption
interception
emulation
encapsulation of malicious content
authentication (mis-authentication)
insufficient inventory of critical components
encryption (prevents observability)

The Blue Box



Steve Jobs and Steve Wozniak in 1975 with a bluebox

- **CCITT#5 in-band signalling sends control messages over the speech channel, allowing trunks to be controlled**
- **Seize trunk (2600) / KP1 or KP2 / destination / ST**
- **Started in mid-60's, became popular after Esquire 1971**
- **Sounds produced by whistles, electronics dialers, computer programs, recorded tones**

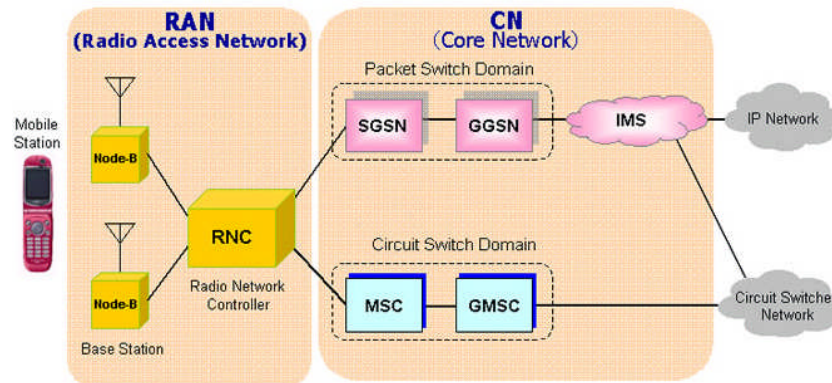


The end of the blueboxing era



- **Telcos installed filters, changed frequencies, analyzed patterns, sued fraudsters**
- **The new SS7 digital signalling protocol is out-of-band and defeats blueboxing**
- **In Europe, boxing was common until the early nineties and kept on until 1997-1998**
- **In Asia, boxing can still be done on some countries. There were blueboxers in KL (at least in 1995-1996)**

Switching Network



- Creation of ghost numbering trees
- Forwarding loops
- Modification of roaming profiles
- Creation of ghosts subscriptions on HLR
- Special CDR (Charging Data Record) generation rules
- DoS / harassment / pranks
- Injected SS7 protocol messages

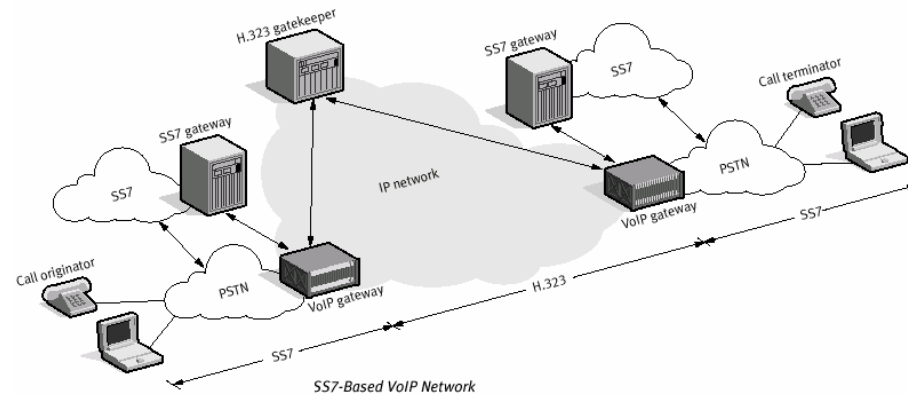
Examples of SS7 attacks

The problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner.

- **Theft of service, interception of calling cards numbers, privacy concerns**
- **Introduce harmful packets into the national and global SS7 networks**
- **Get control of call processing, get control of accounting reports**
- **Obtain credit card numbers, non-listed numbers, etc.**
- **Messages can be read, altered, injected or deleted**
- **Denial of service, security triplet replay to compromise authentication**
- **Annoyance calls, free calls, disruption of emergency services**
- **Capture of gateways, rerouting of call traffic**
- **Disruption of service to large parts of the network**
- **Call processing exposed through Signaling Control Protocol**
- **Announcement service exposed to IP through RTP**
- **Disclosure of bearer channel traffic**

KEY ISSUES in 2007

- Wholesale Fraud
- Fraud with calling card
- SMS Fraud & Security
- SS7 vulnerability – (Hyper-short calls and Voting TV)
- Critical Infrastructure Protection – Boonets
- Threats on E-commerce (including credit card fraud)
- VoIP Fraud & Security + IP PBX HACKING
- Pharming + Phishing
- IRS 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
 - Cooper Cable Theft is a worldwide problem
-

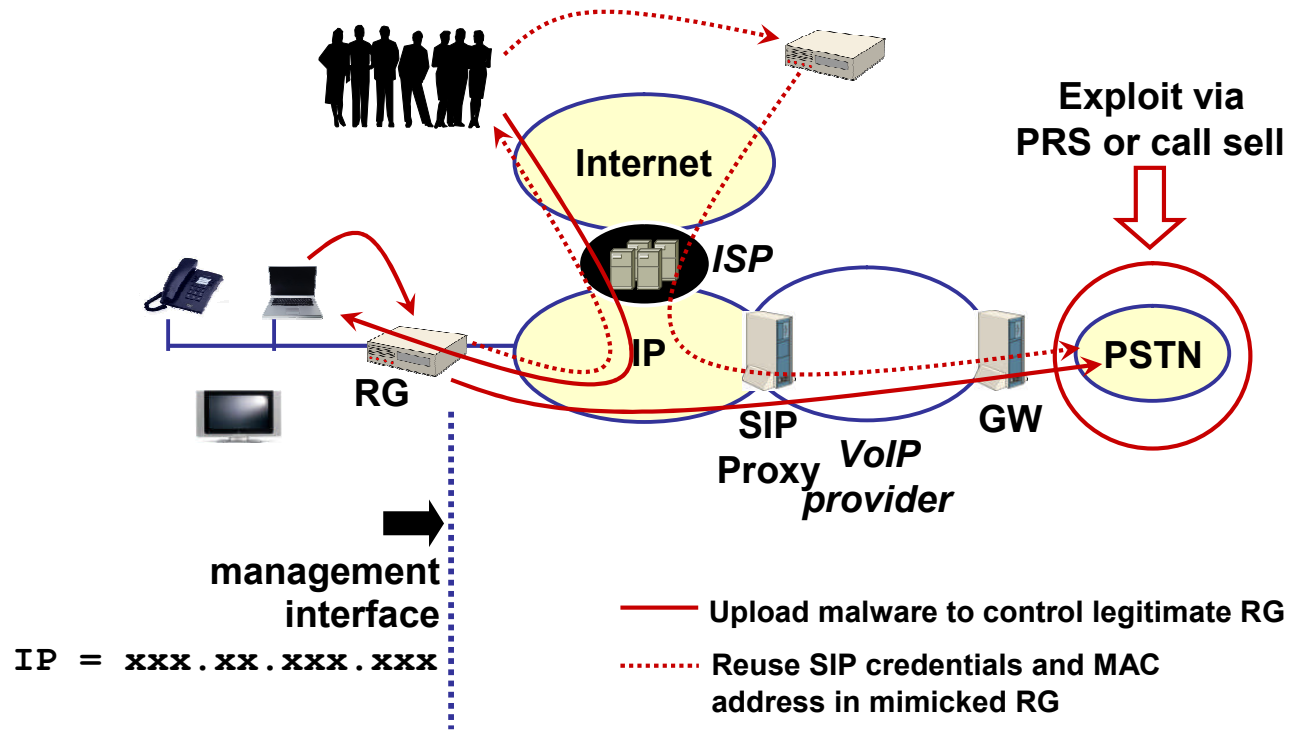


- There is also exponential growth in the use of interconnection between the telecommunication networks and the Internet, for example with VoIP protocols (e.g. SIP, SCTP, M3UA, etc.)
- The IT community now has many protocol converters for conversion of SS7 data to IP, primarily for the transportation of voice and data over the IP networks. In addition new services such as those based on IN will lead to a growing use of the SS7 network for general data transfers.
- There have been a number of incidents from accidental action, which have damaged a network. To date, there have been very few deliberate actions. However, fraud cases are increasing.

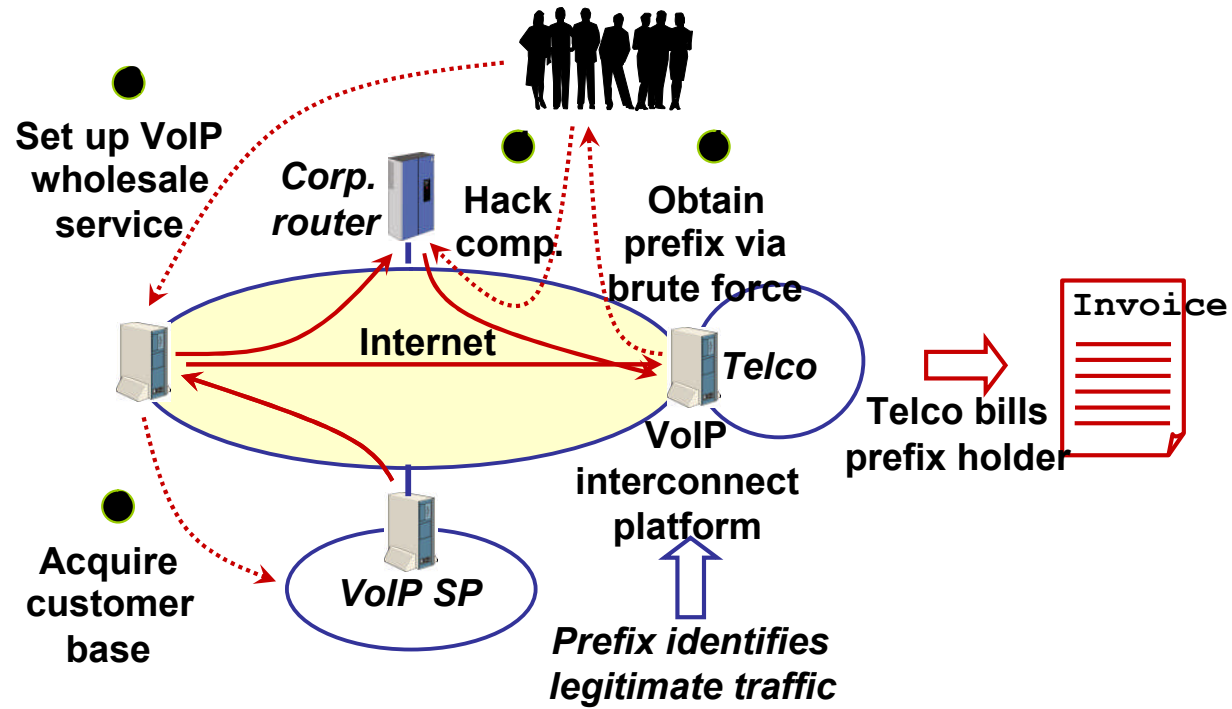
21st century telecom attacks

- **Reseller & Subscription fraud**
- **SIP account hacking**
 - Remember "Calling Cards" fraud?
- **VoIP GW hacking**
 - Remember "PBX hacking"?
- **Signalling hacking directly on SS7 – SIGTRAN level**
 - Back at the good old BlueBox?
 - Not nearly but, the closest so far

New Technology – Residential Gateway Abuse Scenarios



New Actors – VoIP Wholesalers Scenario



How does it affect the backbone?

- **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)

Impact for security

- **Much more people can get their hands on a formerly restricted kingdom**
- **More openness**
- **Expect more innovation to come**
 - **New companies with bright new ideas**
- **Expect more security implication**
 - **Things are not hidden anymore**
- **Expect more need for QA and Security Services**

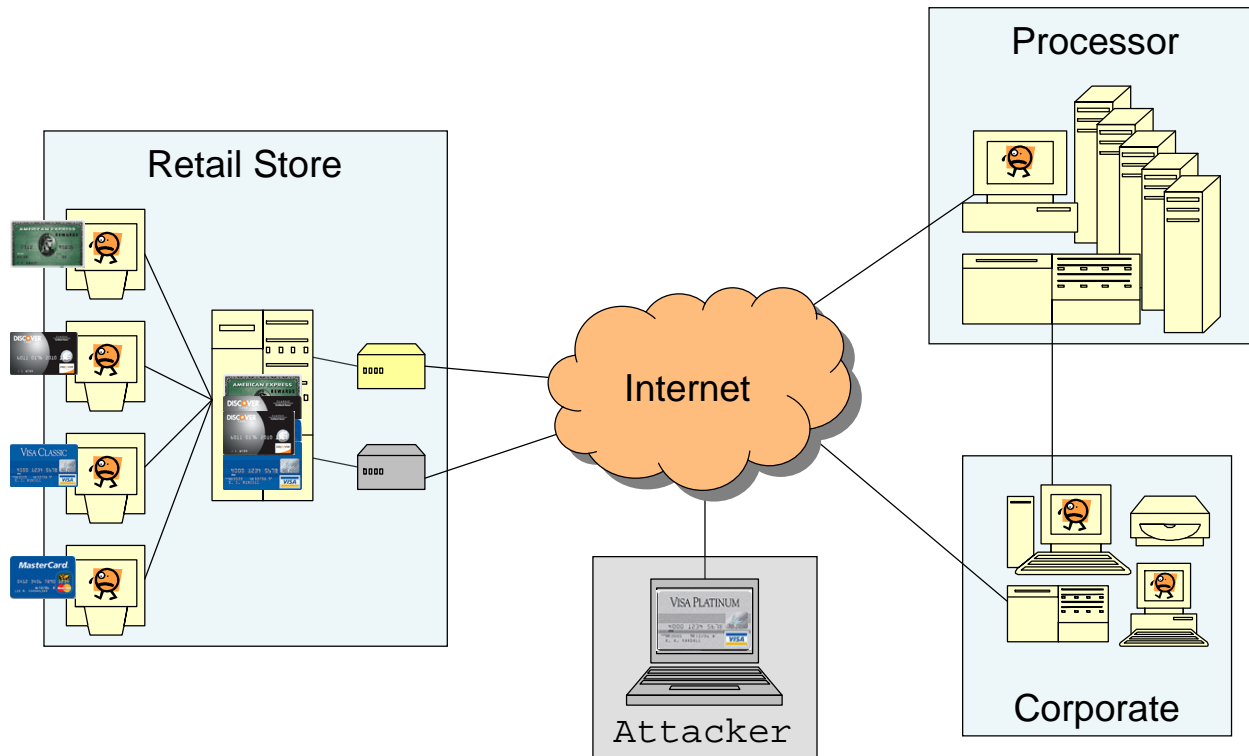
Mobile Security

- **Number of security attacks reported by mobile phone operators in 2006 and 2007 jumped fivefold over the year before**
- **According to data gleaned from more than 200 mobile operators worldwide, 83% said that their subscribers have been hit by some kind of mobile device infection.**
- **Large-scale attacks during 2006 and 2007 were most likely in Europe, Asia and the Pacific Rim. In those regions, the Operators reporting incidents that affected more than 1000 devices doubling during the year.**
- **Attacks involving between 1,000 and 100,000 devices accounted for just 15% of all reported security events.**
- **As mobile data use and functionality proliferates, security is becoming an essential enabler for the success of new revenue-generating services**

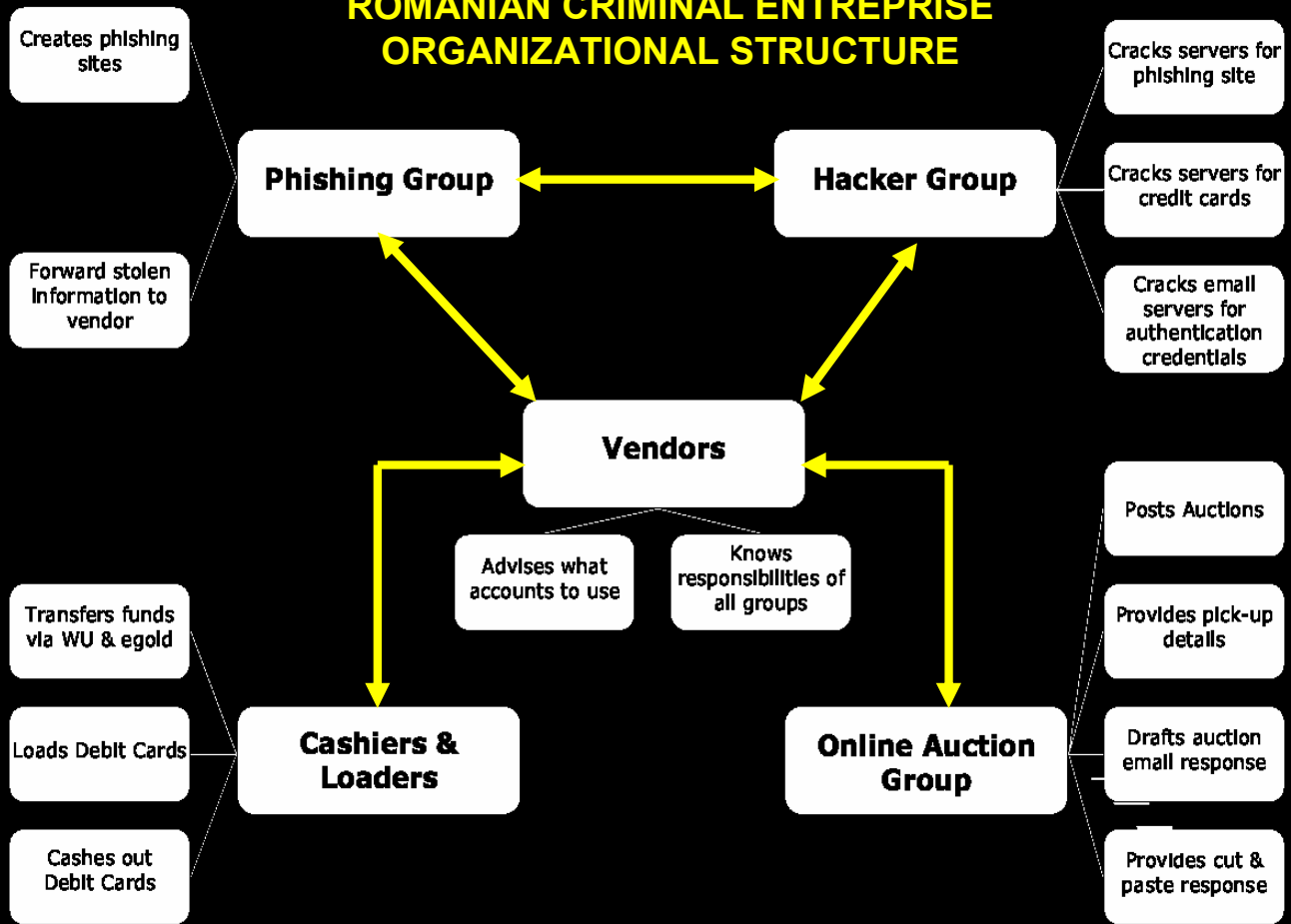
CARDING MAJOR CASE

- **Eastern European Subjects compromised numerous computer networks, stealing data and subsequently extorting the victim companies to ensure silence.**
- **52 cases Consolidated into Major Case.**
- **An estimated thirty million credit card accounts, including personal information were compromised.**
- **The stolen information was released whether victim company paid the subjects through online transfers or refused the extortion demands.**
- **Credit card numbers are often sold online to others for illicit gain Even after stolen information was posted on the web by the subjects, roughly half of the victim companies continued to deny that their networks had been compromised.**
- **Damages are conservatively estimated at 15 billion dollars.**
- **Two subjects lured from Russia. One subject voluntarily surrendered to US Law Enforcement. Two subjects prosecuted in Belarus.**
- **Established continuing relations with Cyber investigators in numerous Eastern European Countries.**
- **FBI targets, Romanian Criminal Enterprise**

Case Study : POS System



ROMANIAN CRIMINAL ENTREPRISE ORGANIZATIONAL STRUCTURE



Botnets and Cyber Crime

- **Criminals controlling millions of personal computers are threatening the internet's future. Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets**
- **Botnets are made up of large numbers of computers that malicious hackers have brought under their control after infecting them with so-called Trojan virus programs.**
- **While most owners are oblivious to the infection, the networks of tens of thousands of computers are used to launch spam e-mail campaigns, denial-of-service attacks or online fraud schemes**
- **The Cyber attack to Estonia was a typical example of botnets use**
- **Dutch prosecutors arrested a trio of young men for creating a large botnet allegedly used to extort a U.S. company, steal identities, and distribute spyware now say they bagged bigger prey: a botnet of 1.5 million machines.**

BOTNET INVESTIGATION



BOTNET INVESTIGATION



Fortress Mentality



The Liability issue

- **Consumers need to know that they may be directly implicated in the criminal activities being perpetrated by botnets – if not by having their own identity or personal information stolen, then by being part of a network of zombie PCs carrying out large scale criminal activities like massive spam distribution and phishing email schemes.**
- **Concerning Network security and the associated liability issues a negligence argument can be made in support of liability for insecure networks. This argument would need to show that the insecure party "had a duty to use reasonable care in securing its computer systems, breached that duty by failing to employ adequate security, and was a reasonably recognized cause of actual damages."**
-E. Kenneally , "Who's Liable for Insecure Networks?" Computer, June 2002,, pp. 93-94.
- **In the new age of broadband computing, home users represent a major source of potential security hazards. Should home users be liable if they do not take certain steps (e.g., apply software patches, install a firewall, or use antivirus software) to secure their computers?**



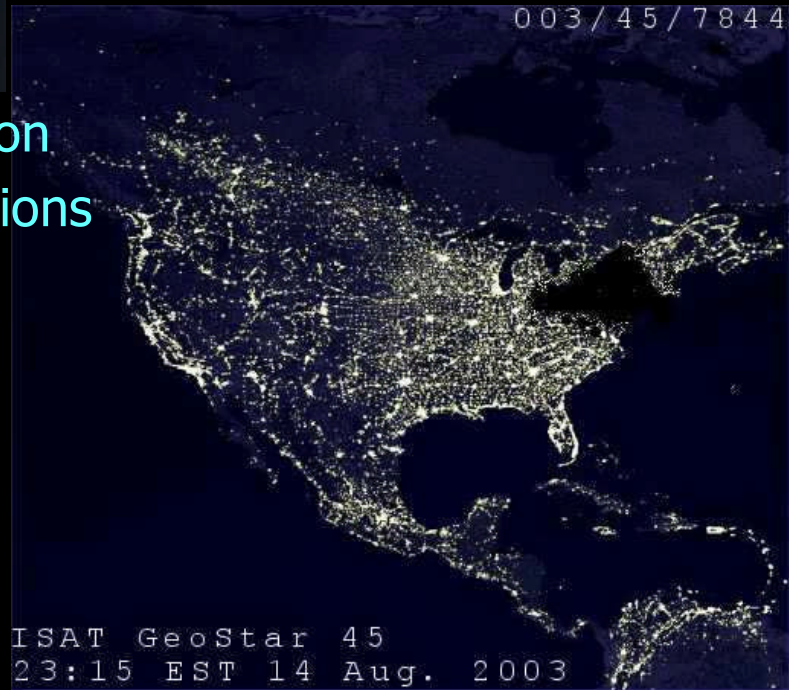
DoS

- Transportation
- Communications
- Power
- Financial



003/45/7844

ISAT GeoStar 45
23:15 EST 14 Aug. 2003




The Rising of Outsource

- **Rising Use of Outsourced Services Equals More Rigorous Security Controls**
 - It is commonplace to see functions such as payroll, human resources, and accounting handled by external firms. Service providers have more recently, moved into hosting and managing e-mail, websites and even corporate IT infrastructures. This model, while cost effective, requires more stringent legal, process, and technical controls to ensure that the service provider does not exploit the powerful access it is given. Prudent organizations are evaluating the security risks associated with outsourcing and are designing process controls and implementing technology configurations that provide transparent administration and audit records.

Organized crime and Call Centres

It has been noted that Organized Crime is infiltrating members in call centres to pass along sensitive personal information

- ❑ Police in Strathclyde, Scotland, said that 10% of call centres in Glasgow have been infiltrated by Organized crime gangs looking for commit fraud. Glasgow is home to roughly 300 call centres employing more than 18000 people.**
- ❑ It has been reported that in several cases of IT theft the private information was stolen in Call Centres in India (e.g. twelve people have been arrested for cheating Citibank customers out of \$350,000. Three of the men worked for Mphasis, an offshoring firm which runs call centres in Bangalore and Pune).**



WIN REAL MONEY!

[Click here!](#)

Recent Winners:
Dylan B. WON \$357,508.00

[I Agree! Play Now!](#)

DEPOSIT **\$100**
 & GET **\$100 FREE!**

[CLICK HERE!](#)

EXCITING NEW SOFTWARE

20% Bonus
 on your first Deposit.



[DOWNLOAD](#)

BET ON BASKETBALL PLAYOFFS

INTERCASINO **\$90 FREE BONUS**

[> click here <](#)

Free Casino Bonus Money
[Click Here!](#)




















We welcome the above secure and simple purchasing methods

ONLINE GAMING

- ❖ **Online games are those that are played online via the LAN, Internet or another telecommunications service.**
- ❖ **Normally, all technical requirements for playing online games is a web browser and/or appropriated client software.**
- ❖ **The general designation of this games is MMORPG – Massive Multiplayer Online role-playing Game.**
- ❖ **Along with the growth of information technology, online gaming has become a very successful and outstanding industry**
- ❖ **According to the DataMonitor.com, the global online gaming market represented \$3.2 billion and 113 million users in 2005**
- ❖ **The success of online gaming changes the software business model, and makes the related industry have a prosperous growth, for example, broadband network, online payment, internet café, advertising and so on.**
- ❖ **It also impacted the Internet business model.**

Gambling and Games

- Lottery
 - Scratch-its
 - Megabucks
 - Powerball
 - Video gaming
 - Keno
 - Bingo
 - Casino gaming
 - Strategic Games
-  **Sports bets**
 -  **Horse racing**
 -  **Stocks**
 -  **Internet**
 -  **Office pools**
 -  **Poker/cards**
 -  **Bets among friends**

 -  **MMORPG** (massively multiplayer online role-playing game)

VIRTUAL PROPERTY

❖ There is market place for virtual properties

- In MMORPGs, players have to pay a network connection fee for operating their virtual character; in the meanwhile, related valuable virtual parameters accumulate. Since the number of virtual properties is limited and some virtual equipment cost time and energy to develop, some players who strongly desire these assets would like to trade for them. This causes has created a marketplace for virtual properties.
 - In the online game, the Lineage II, a UserID for someone who has reached the 57th level in the game is valued at \$2000 U.S. dollars in an Ebay auction website.
 - In ItemBay.com, more than 21,907 related virtual properties of online gaming were sold, bought, or bid for in a an auction website.
 - A virtual dragon knife received a bid of \$4,800 U.S. while a royally invincible claw received a bid of \$4,270 recently.
 - Even the virtual currency in an online game can be converted into cash through exchange with other players. The virtual currency exchange rate was 2500:1 (2500 virtual currency can be converted to 1 US dollar) in March 2003.

These facts indicate that virtual property trading is indeed prosperous and flourishing

VIRTUAL PROPERTY

- ❖ **Trading of virtual property has become part of the entertainment pleasure, experience, and is now common practice.**
- ❖ **When virtual properties become valuable in the real world, an online game can involve more than just entertainment.**
- ❖ **The involvement of real money can easily lead to conflicts and criminal behaviours.**

KNOWN CASES OF CRIMINAL BEHAVIOUR

- **In China-Taiwan One girl was defrauded about US\$ 42,000 through her virtual property trading**
- **One report from Hankyoreh.com of South Korea mentioned that a cheater, who was caught in May 2001, had earned more than US\$ 11,000 by cheating in online gaming**
- **Virtual properties belonging to twenty players were stolen in an Internet café simultaneously due to UserID and password hacking**
- **Offenders kidnapped two players and force them to disclose their UserIDs and passwords; afterwards, they stole all the virtual properties belonging to their victims**
- **Police hunted down an offender who developed and distributed illegal cheating programs in China and found over 30,000 detailed UserIDs and passwords**



**ORGANIZED
CRIME
DECIDE TO
PLAY**

BLACKMAIL & DoS

**On-line gambling is the wild west
of the gaming world.**

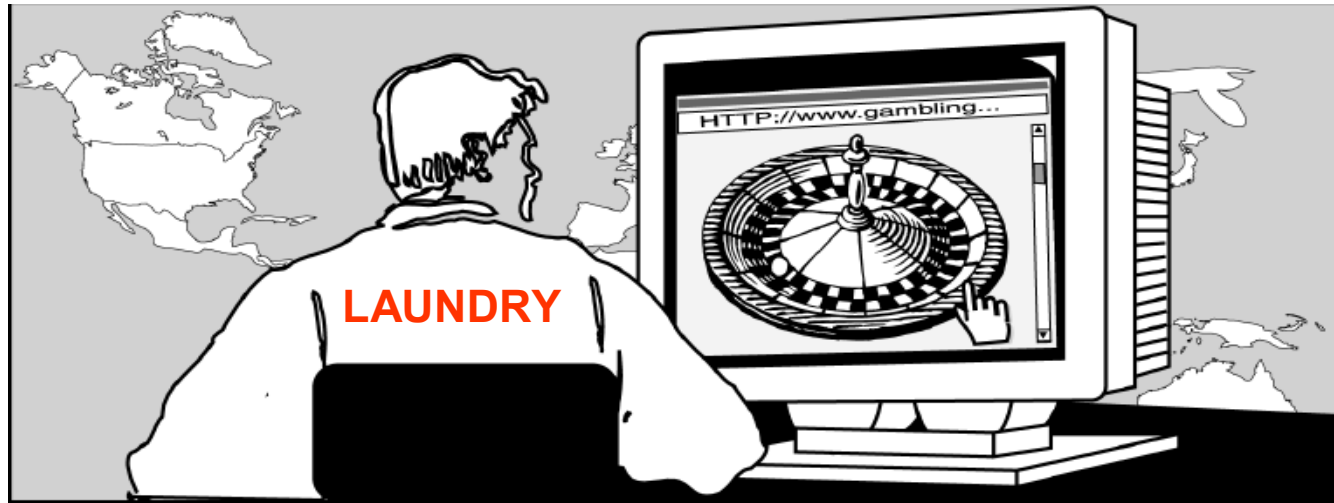
It is a multi-billion dollars industry.

According to law enforcement agencies, there are numerous reports of organized crime operations from Russia and Eastern Europe carrying out denial-of-service (DOS) attacks, to blackmail online gambling sites and e-commerce websites.

Extortion At Online Casinos In Three Easy Steps

- 1. Crime rings distribute viruses to tens of thousands of unprotected computers, which turn them into armies of so-called zombies that the extortionists then control.**
- 2. They orchestrate these zombies to send blizzards of messages to an online casino's Web site. These slow traffic to a crawl, giving casino operators a taste of the extortionists' power.**
- 3. In ransom e-mails to casino operators, they threaten to shut down the site with massive attacks just before big events. Cost to stay up and running: \$30,000 to \$60,000.**





Internet gambling can be a significant vehicle for laundering criminal proceeds, especially to move illicit funds among financial institutions at the layering stage. The officials said that the volume, speed, and international reach of Internet transactions and the fact that many Internet gambling sites are located offshore increased the potential for misuse.



ONLINE GAMING & SECURITY

- ❖ **More and more ways of cheating along with the accompanying criminal Behaviours have been struck against our society and the computer gaming industry.**
- ❖ **Along with the success of online gaming, the negative influences of online gaming have become a serious issue to our society. It has not only increased the number of different types of criminal activities, and has also led to an increase in traditional crime. Though these new criminal problems do not appear to be as serious as conventional violent crimes, people still need to be aware of them.**
- ❖ **Network gaming is emerging as one of the most exciting areas in the computer gaming industry.**
 - ❑ **Opportunity for small and large developers to deliver new products and services**
- ❖ **Security is a critical requirement to accelerate the growth and ensure the success of this industry.**
- ❖ **Two main security goals for online games:**
 - ❑ **Protecting sensitive information (e.g., credit card numbers)**
 - ❑ **Providing a fair playing field (i.e., making cheating is as difficult as possible)**

Only a minority of cheaters try to create open and immediate havoc, whereas most of them want to achieve a dominating, superhuman position and hold sway over the other players.

Telecommunication fraud

HOW DOES ONE MAKE THE BUSINESS IMPACT OF FRAUD CASES VISIBLE FOR MANAGEMENT??

CFCA/FIINA:

3 % of the telco's annual turnover is lost because of fraud.



Surveys on Fraud Losses

- **Average fraud loss for ETNO Members is equal to 0.75% of Revenue (Turnover). Many of ETNO Members have multi-national operations. 78% of ETNO Members have prepay products and only 57% of them have had fraud on these type of products**
- **TNO researchers to Dutch Ministry of Justice reported that to Western Europe Operators the fraud losses are usually less than 1% of the turnover. It also said that in general the ratio fraud losses/revenues are in Western Europe 1/3 of the ratio for worldwide operators.**
- **An independent research was carried out by Analysys for Subex Azure between May and July 2007. In this survey is reported that the average “acceptable” level of loss is 1.8% of revenues. However, major incumbents were least tolerant (1.2%). The worst affected regions are Middle East and Africa, Asia Pacific and Central and Latin America and that Mobile operators have higher levels of loss than incumbent and altnet wireline operators**

Cyber Crime can have a huge impact on business bottom line

	<i>Australia</i>	<i>Japan</i>	<i>India</i>	<i>Global</i>
Loss of revenue	71%	81%	75%	72%
Loss of market capitalization	68%	75%	72%	47%
Damage to brand/reputation	67%	73%	65%	63%
Loss of current customers	58%	57%	64%	67%
Loss of employee productivity	57%	55%	60%	47%
Loss of prospective customers	46%	44%	57%	38%
Cost of restoring service	43%	39%	53%	52%
Cost of notification to customers, suppliers, and general public	41%	37%	24%	28%
Cost of investigating breach	31%	23%	22%	43%
Legal fees	18%	16%	8%	22%
No response	-	-	-	1%

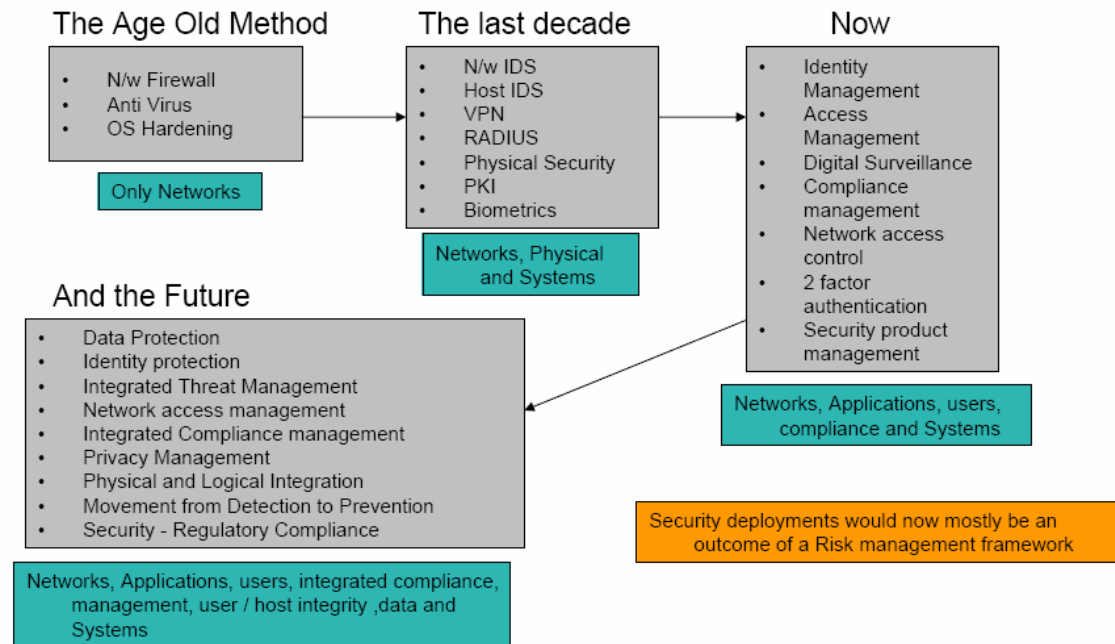
Source: IBM Global Security Survey

Economic Impact of Cyber Crime

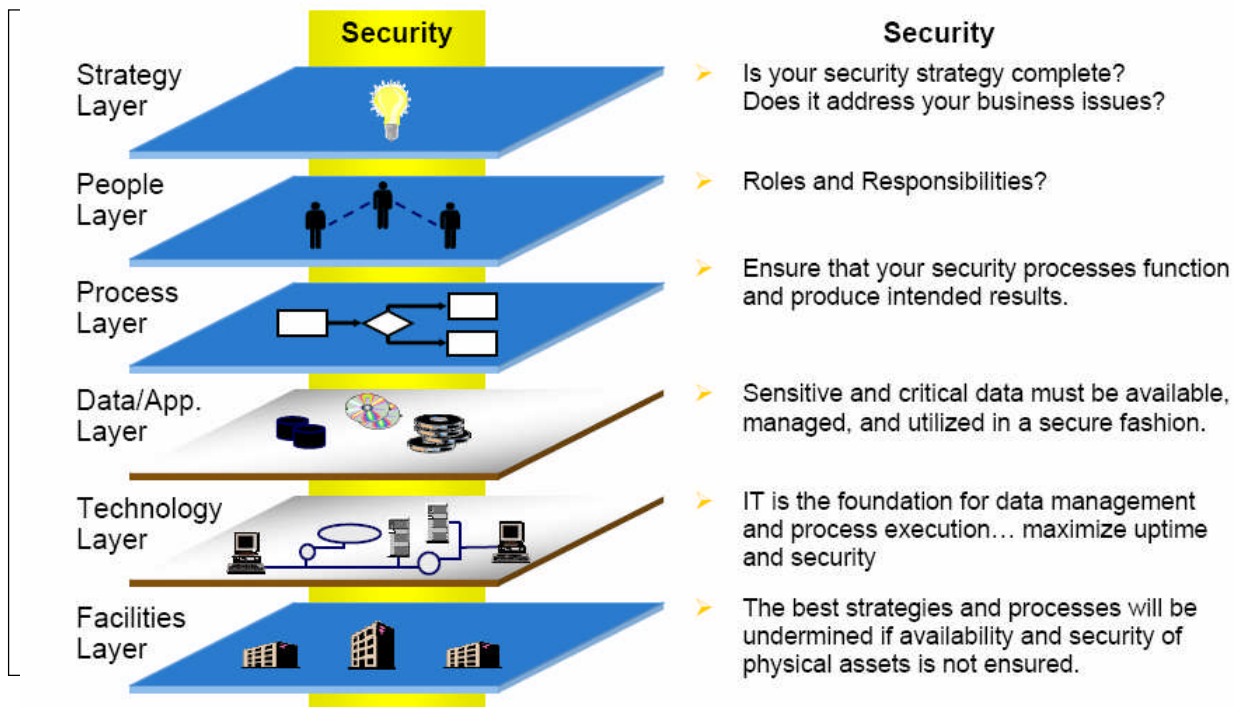
Examples of the impact of cyber crime

- Diminished consumer confidence**
- Lost productivity**
- Loss of trade secrets**
- Refused access to certain markets**

SECURITY EVOLUTION



SECURITY is a TOP-DOWN APPROACH

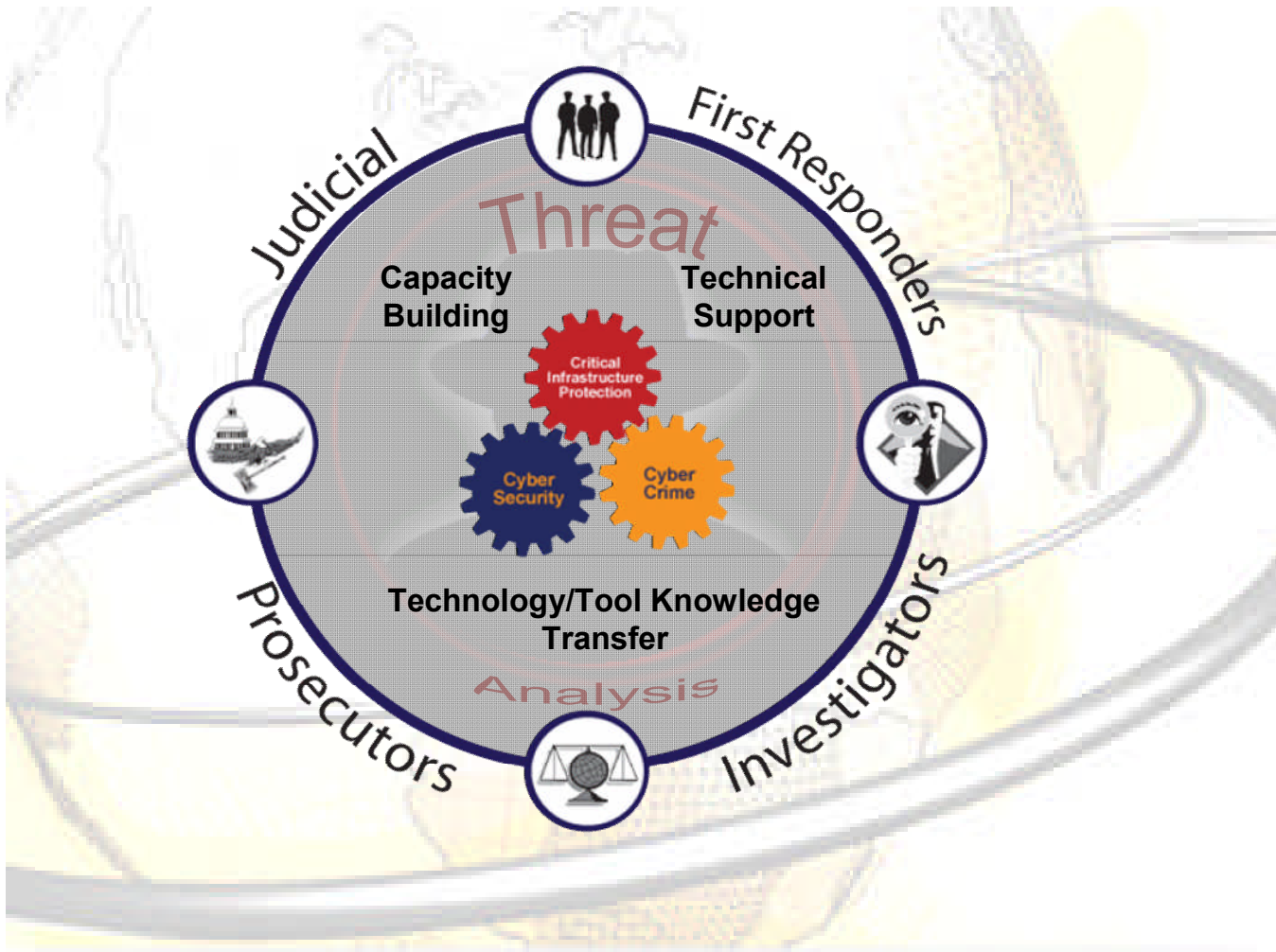


Some Conclusions

- **Potential for the reduction in fraud management department sizes and very few Telecom Security specialists (Even less people legacy (SS7) security expertise)**
- **Lack of preparation for VOIP, IP, & IMS**
- **Need to review the position of FM Team in Organisation subject area (financial vs technical)**
- **Inadequately configured and under-sized systems**
- **Many existing systems will struggle to handle IP information**
- **Pricing of IP services not logical in relation to fraud risk**
- **Lack of cooperation from outside Europe region.**

Through systematic and careful planning, the proper policies, laws, regulations and awareness can help mitigate the threat

Success depends on various key stakeholders and policies, law must be enacted and enforced by government, Parliament, industry and individuals



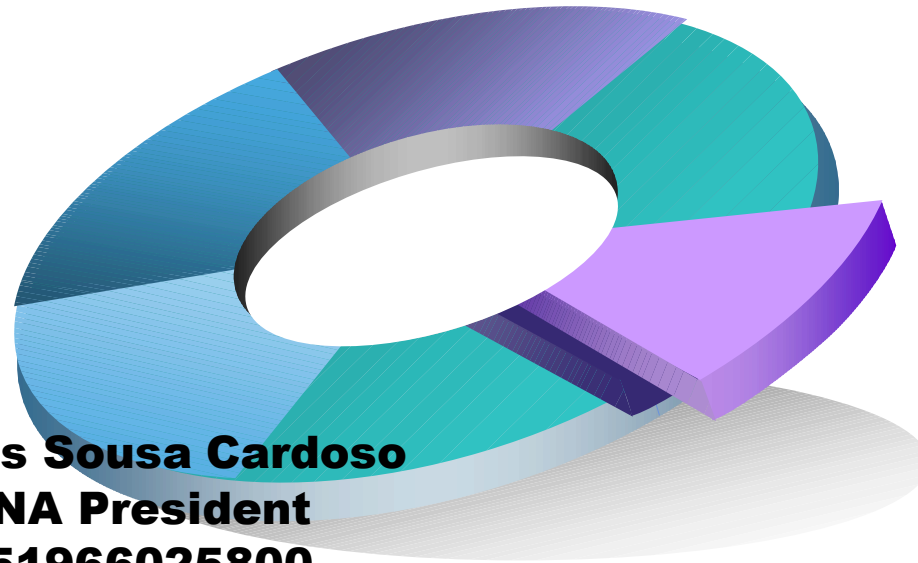
Summary: Dangers are Lurking...

“Only the paranoid survive”

- Andy Grove



More Information...



Luis Sousa Cardoso
FIINA President
+351966025800
LuisSCardoso@ieee.org