



# Aspetos Profissionais e Sociais da Engenharia Informática

Security issues and challenges

Rui L Aguiar, UA/IT

1

## Covered aspects....

- AI
  - Market, technology, what is “IA”
- Open source models, trabalhos derivados
- Marcas, IPR
- Standards
- Dilemas de personalidade – tempo e constância.
- Applied AI issues: autonomous driving and decisions

2

2



## Today....

- Cybersecurity – what is it and what is the impact
- Cybercrime
  - Employment and information leakage
- Reputation
- Legal intercept
- Cybermarket

3

3



# CYBERSECURITY

4

2



## Importance of Cyber Security



■ “The only system which is truly secure is one which is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn’t stake my life on it.”

■ Gene Spafford

- There is nothing like absolute security
- We are only trying to build comfort levels, because security costs money BUT lack of security may cost much more
  - Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations
- Challenge:
  - security has clear costs, while lack of security may have cost

5



## Cyber Security Defined

- Cyber Security's goal: **Protect our information and information systems**
- Cyber Security is: “**Protection** of information systems **against unauthorized** access to or **modification** of information, whether in storage, processing or transit, and against the **denial** of service to authorized users, including those measures necessary to detect, document, and counter such threats.”
  - This version is very reductionist: ICT is now merged with society, so in reality we are talking about protecting assets.

**\$1 Trillion Has Been Spent Over  
The Past 7 Years On Cybersecurity,  
With 95% Success ... For The Attackers**



46% say they can't prevent attackers from breaking into internal networks each time it is attempted.



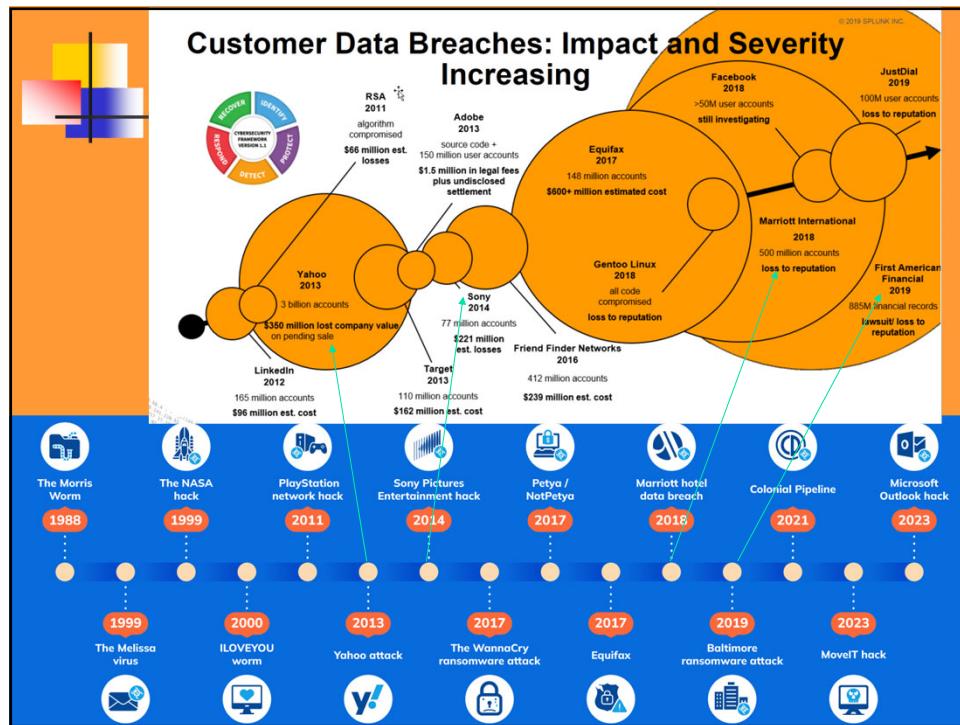
100% of CIOs believe a breach will occur through a successful phishing attack in next 12 months.



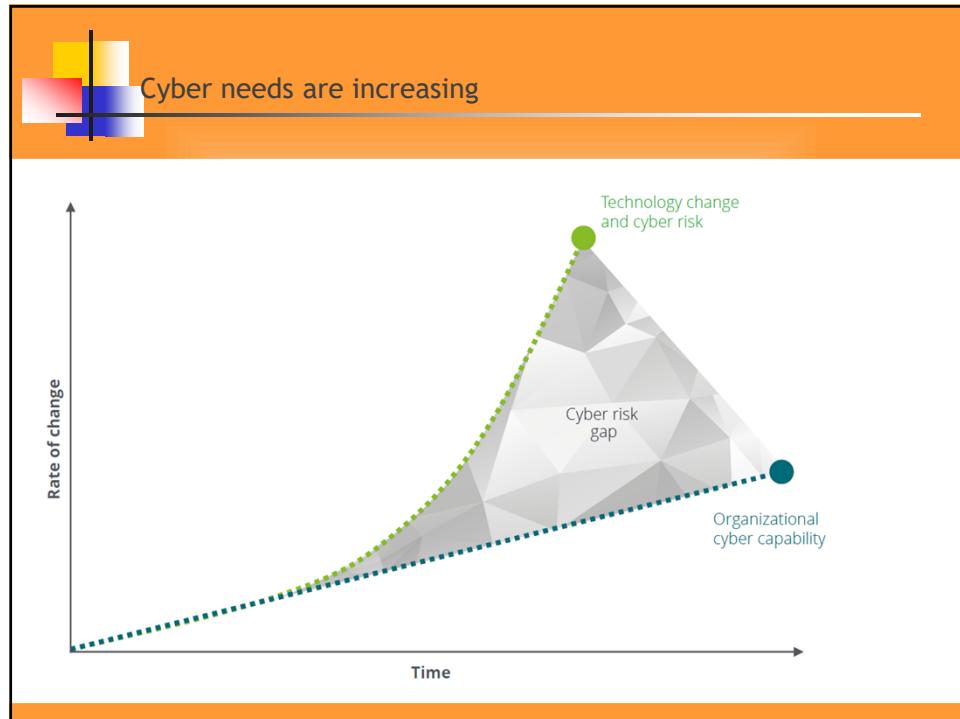
Enterprises have seen a 26% increase in security incidents despite increasing budgets by 9% YoY.

6

6



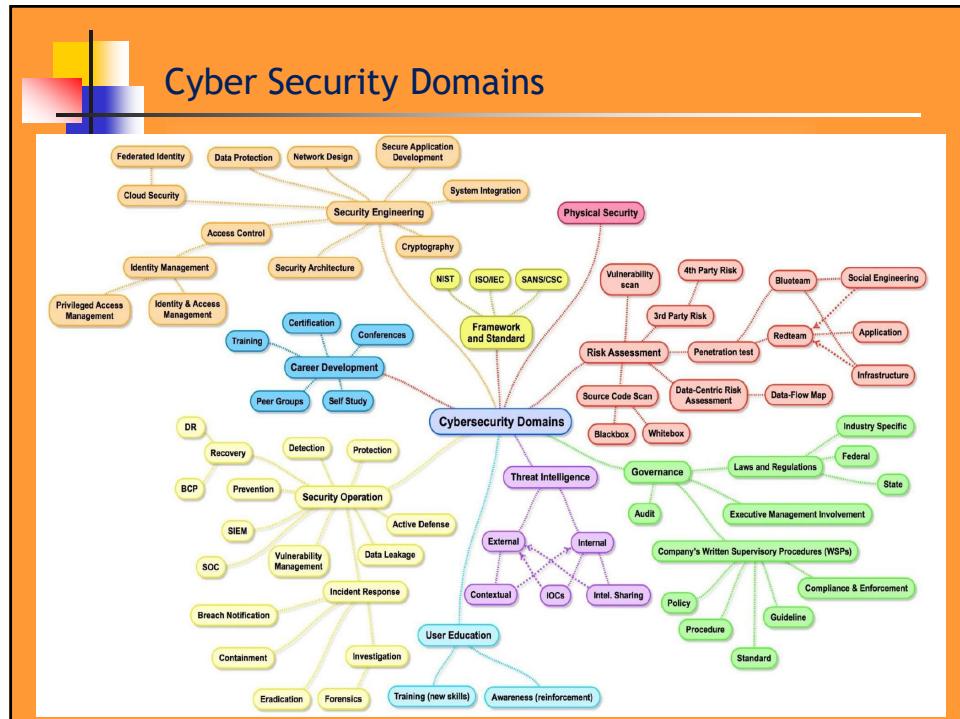
8



9



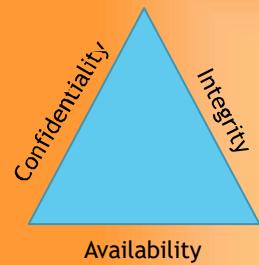
10



11



## Recall: What is a Secure System? (CIA Triad)



- **Confidentiality** - restrict access to authorized individuals
- **Integrity** - data has not been altered in an unauthorized manner
- **Availability** - information can be accessed and modified by authorized individuals in an appropriate timeframe

12



## Recall: Sensitive Data

- Information is considered **sensitive** if the **loss** of **Confidentiality**, **Integrity**, or **Availability** could be expected to have a **serious**, **severe**, or **catastrophic** adverse **effect** on organizational operations, organizational assets, or individuals.
- **Types** of sensitive information include:
  - Personnel
  - Financial
  - Payroll
  - Medical
  - Privacy Act information.
- This definition does not clarify **the separation between company and legal considerations**. Some sensitive data is *legally* sensitive, other is *corporate business* sensitive.

13

13

## Phishing and Spear-phishing Attacks

### WHAT KINDS OF THREATS ARE THERE?

- Social Engineering Scams
- Common Malware and Ransomware
- Business Email Compromise
- Fake websites that steal data or infect devices
- And much more

**The Inevitability of the Click**

E-mails Per Campaign	Probability (%)
2	20
4	60
6	85
8	95
10	98
12	99
14	99.5
16	99.8
18	99.9
20	100

**MASS-SCALE PHISHING**  
Attack where fraudsters cast a wide net of attacks that aren't highly targeted

**SPEAR PHISHING**  
Tailored to a specific victim or group of victims using personal details

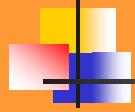
**WHALING**  
Specialized type of spear phishing that targets a "big" victim within a company e.g., CEO, CFO, or other executive

14

## Setting an Exploit Kit

15

## Identity Theft



- Impersonation by private information
  - Thief can 'become' the victim
- Reported incidents rising
- Methods of stealing information
  - Shoulder surfing
  - Snagging
  - Dumpster diving
  - Social engineering
  - High-tech methods
- Loss of privacy
  - Personal information is stored electronically
  - Purchases are stored in a database
    - Data is sold to other companies
  - Public records on the Internet
  - Internet use is monitored and logged
  - None of these techniques are illegal



16

## Example Attack: Business Email Compromise



**Step 1:**  
Identify a Target



Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

**Step 2:**  
Grooming



Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department). Perpetrators use persuasion and pressure to manipulate and exploit human nature. Grooming may occur over a few days or weeks.

**Step 3:**  
Exchange of Information



The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

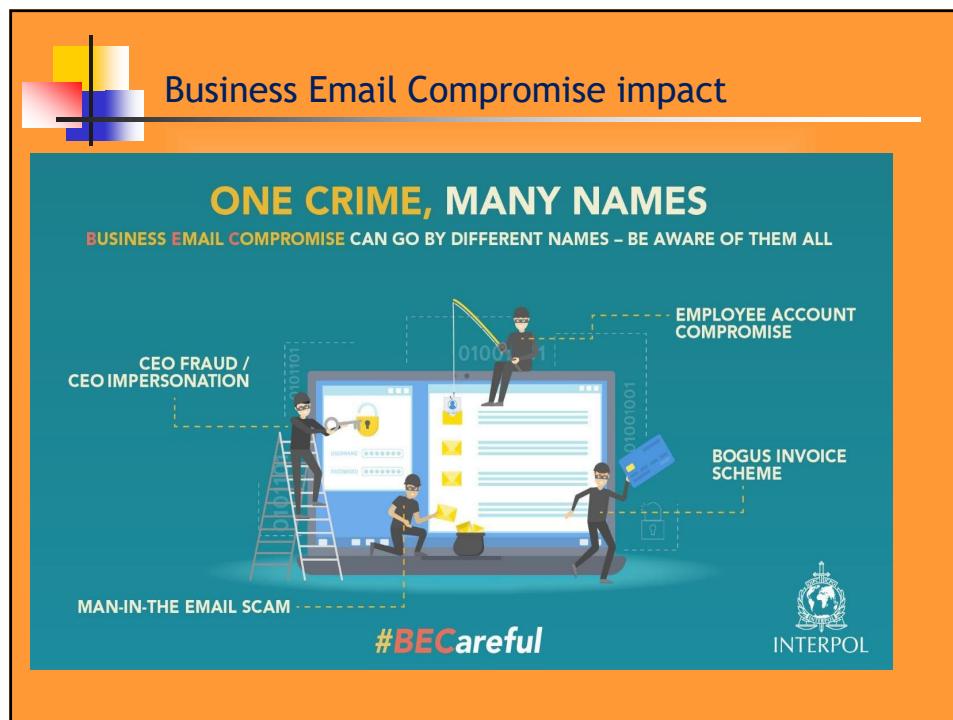
**Step 4:**  
Wire Transfer



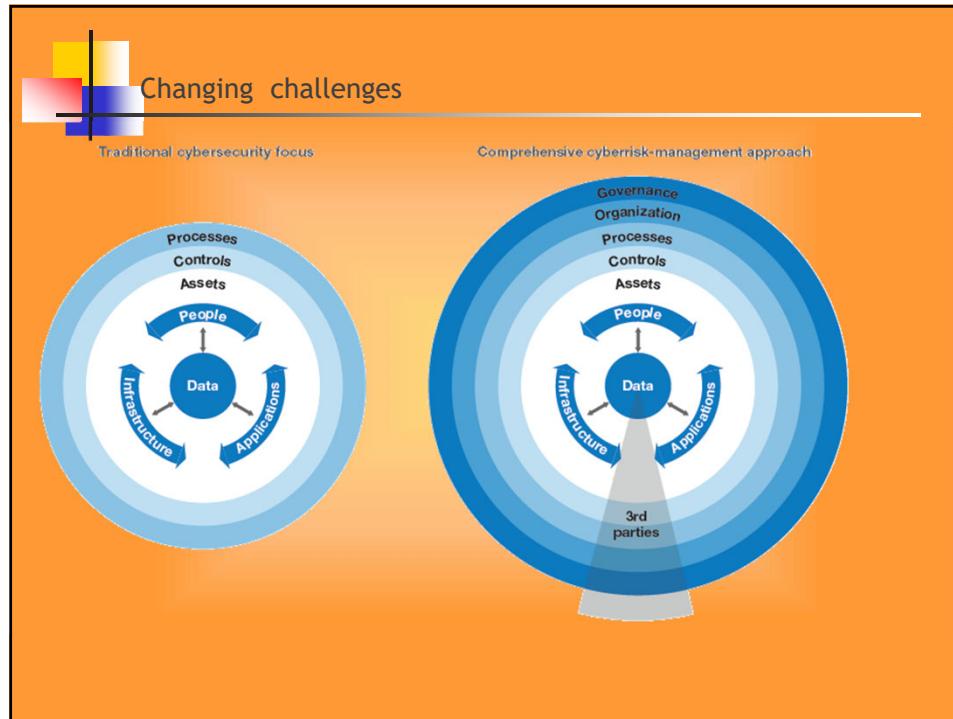
Upon transfer, the funds are steered to a bank account controlled by the organized crime group.  
\*Note: Perpetrators may continue to groom the victim into transferring more funds.

**■ Business E-Mail Compromise Timeline**  
An outline of how the business e-mail compromise is executed by some organized crime groups

17



18



19



20



21

## Cyber Crime

Cyber Crime is a generic term that refers to all criminal activities done using the medium of communication devices, computers, mobile phones, tablets etc. It can be categorized in three ways:

- **The computer as a target** – attacking the computers of others.
- **The computer as a weapon**- Using a computer to commit “traditional crime” that we see in the physical world.
- **The computer as an accessory**- Using a computer as a “fancy filing cabinet” to store illegal or stolen information.

22

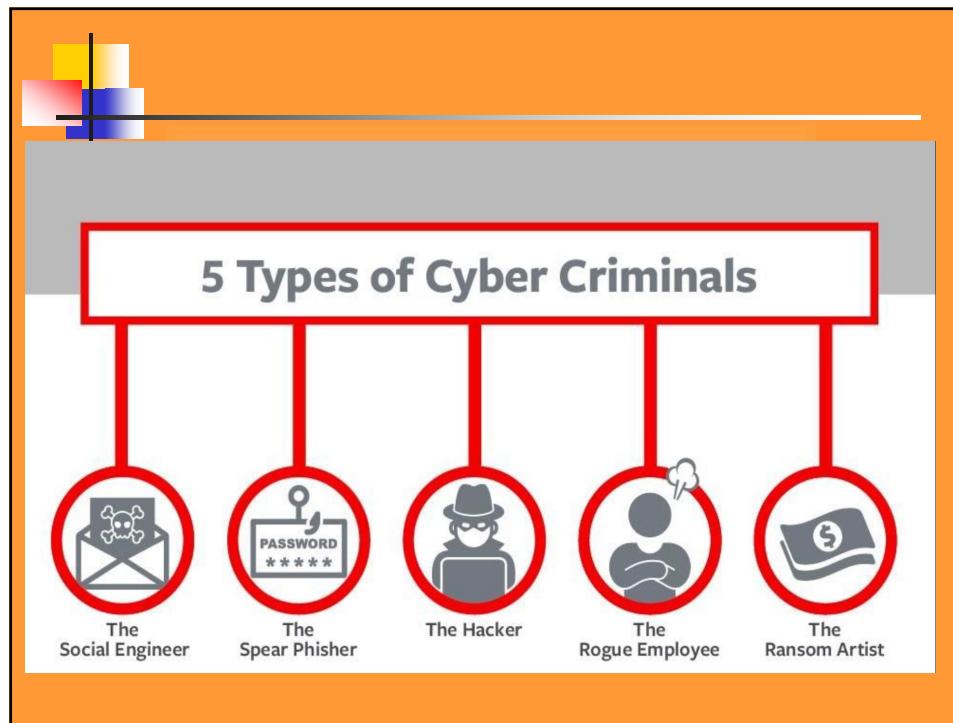
## Types of Cybercrime

The chart is a donut chart with ten segments, each representing a type of cybercrime. The segments are color-coded and labeled as follows:

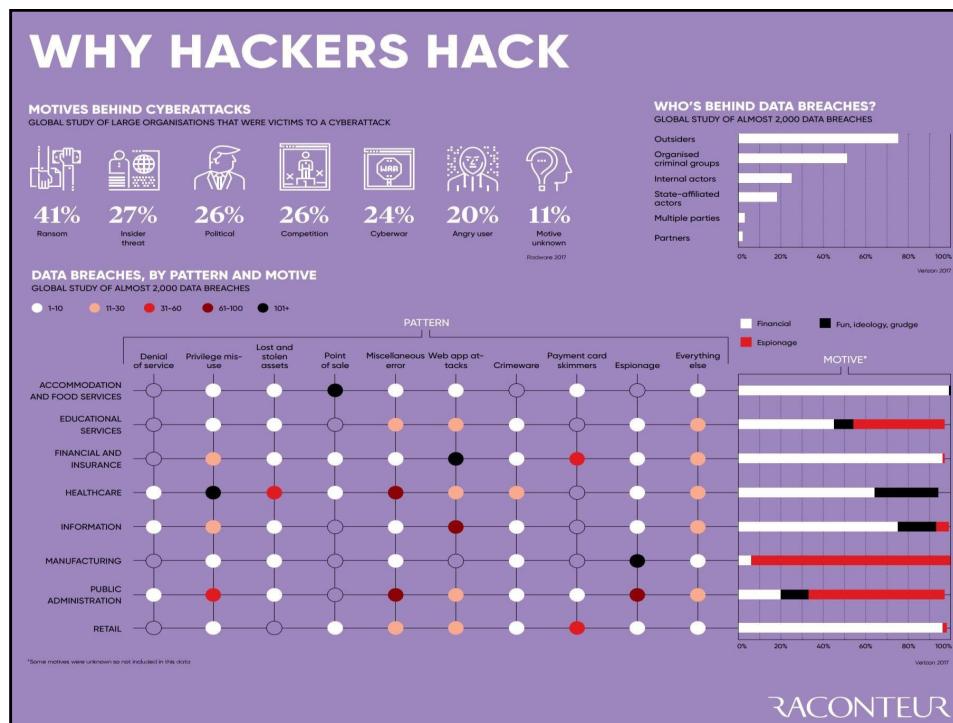
- Online scams
- Identity theft
- Botnets
- Cyberstalking
- Social engineering
- Flood attacks
- Potentially unwanted programs
- Exploit kits
- Phishing attacks
- Illegal content

SecurityTrails

23



24



25

**Cybercrime as a Service**

**No.1**

**THE RISE OF CYBER-CRIME AS A SERVICE**

**Cybercrime as a-Service Is a Top Threat**

Exploit kits (toolkits for hire that make cyber-crime easier by automating the creation and delivery of malware) remain the biggest threat. They account for 50% of the index.

**CIO INSIGHT**

26

**Cybercrime as a Service costs**

SERVICE	BITCOIN <small>(Typical price range listed along with the highest listed price)</small>	USD <small>(Typical price range listed along with the highest listed price)</small>
HACKING WEB SERVER (VPS OR HOSTING)	0.034 - 0.0449, 0.47	\$220 - \$500, \$3,000
SETTING UP KEYLOGGER	0.0263	\$170
DDOS (PRICES MAY VARY)	0.0534, 0.078 - 0.39	\$350, \$500 - \$2,500
HACKING PERSONAL COMPUTER	0.0364, 0.044 - 0.55	\$280, \$500 - \$3,500
HACKING CELL PHONES	0.047 - 0.093	\$300 - \$600
EMAIL HACKING	0.078 - 0.12	\$500 - \$800
SOCIAL MEDIA ACCOUNT HACKING	0.0352, 0.054 - 0.11	\$230, \$350 - \$700
CHANGE SCHOOL GRADES	0.19 - 0.58	\$1,200 - \$3,750
FUD RANSOMWARE + DECRYPTER	12 MO / 0.14 6 MO / 0.076 1 MO / 0.019	12 MO / \$900 6 MO / \$490 1 MO / \$120

27

## Web, Deep Web & Dark Web

**Surface Web** is only the Tip of the Iceberg

The diagram shows a large iceberg floating in water. The visible portion above the surface is labeled "5 %". The submerged portion below the surface is labeled "95 %". A small boat with the word "traversals" is shown near the surface. The iceberg is divided into three horizontal sections: "SURFACE WEB" (top), "DEEP WEB" (middle), and "DARK WEB" (bottom).

Section	Description
SURFACE WEB	Google, Yahoo, Naver, Yandex, Wikipedia, Reddit, ...
DEEP WEB	Cloud Storage, Patent Data, Research Articles, Legal Documents, Financial Records, ...
DARK WEB	Onion Sites, Hidden Marketplaces, Anonymous Journalism, ...

28

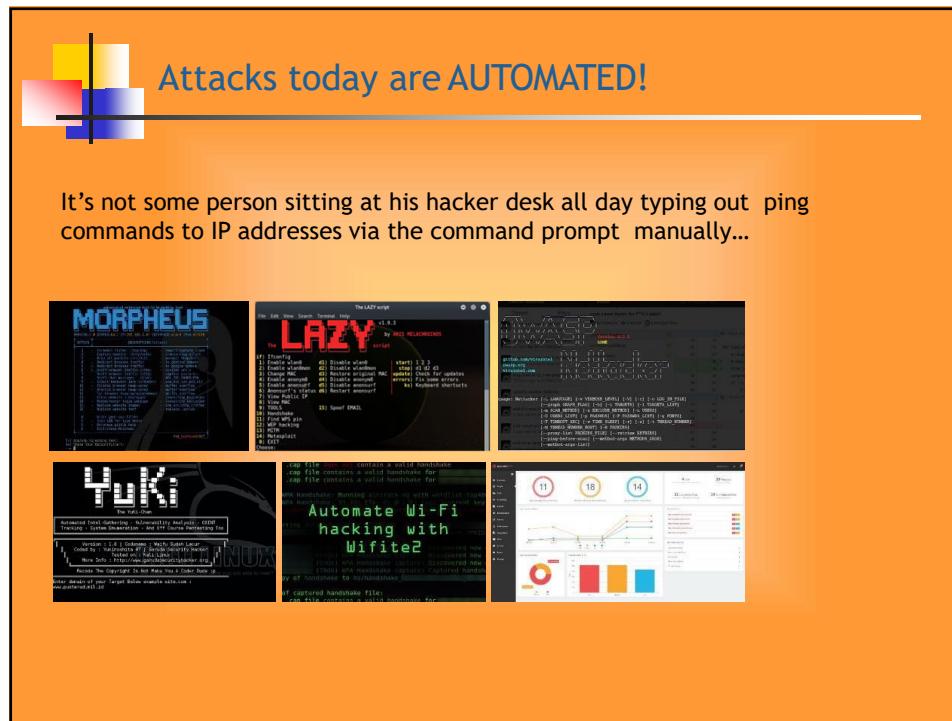
## Global Cyber Security Trends

Recent studies reveal three major findings:

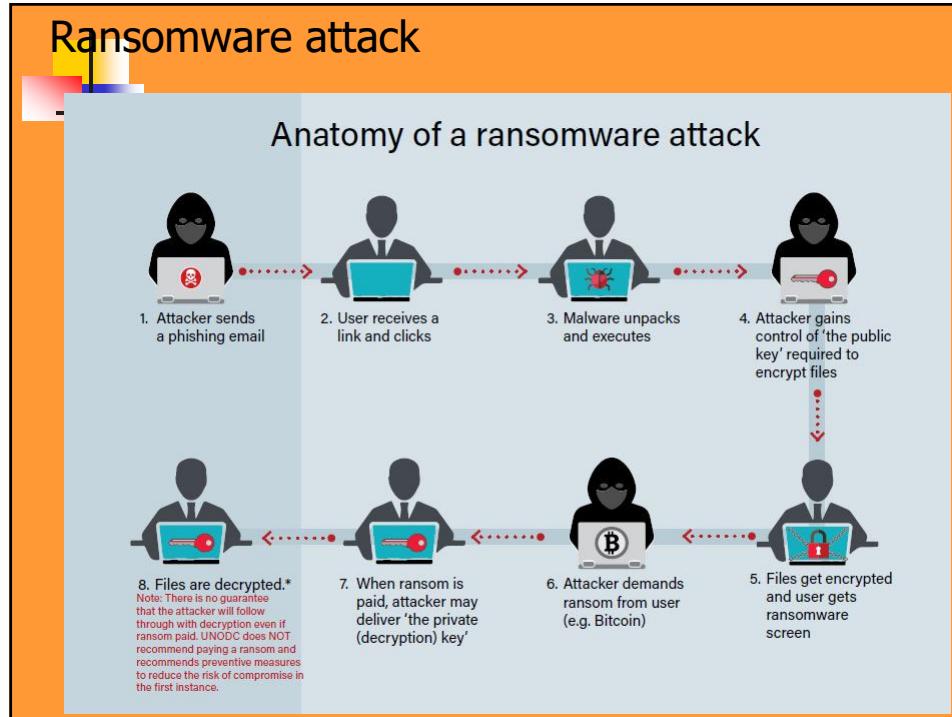
- **Growing threat to national security** - web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organized operations aimed at not only financial, but also political or technical gain
- **Increasing threat to online services** - affecting individuals and industry because of growth of sophistication of attack techniques
- **Emergence of a sophisticated market for software flaws** - that can be used to carry out espionage and attacks on Govt. and Critical information infrastructure. Findings indicate a blurred line between legal and illegal sales of software vulnerabilities

*Mischiefous activities in cyber space have expanded from novice geeks to organized criminal gangs that are going Hi-tech, to state-level actors (funded cyber groups)*

29



30



31

**Event and response**

- PII Personally identifiable information**

- 1 Insider takes sensitive data via flash drive**  
A disgruntled employee installs indexing malware in corporate systems and transfers files from servers to USB drive.  
**Visible hints**
  - Inquiry is made to senior executives about temp file being created and deleted.
  - Slow laptops are reported to IT department and chief information officer.
  - Help-desk ticket is sent to IT security lead.**Typical response**
  - Initially, the IT-security team does not realize that data are being threatened.
  - Once the data are breached, the security team tries to determine best way to inform senior executives; the process is ad hoc, because protocols are not clear.
- 2 Insider gives or sells employee data to a cybercriminal**  
Cybercriminal uses old but valid credentials to access company servers and download employee records containing personally identifiable information (PII).  
**Visible hints**
  - Data-loss alerts are sent to the security lead in the IT organization.**Typical response**
  - Team focuses on the forensics of the alert but is not able to connect it to previous notifications.
- 3 Cybercriminal sells PII data to identity thieves on the black market**  
Identity thieves buy and use the employee data for fraudulent transactions.  
**Visible hints**
  - Based on individuals' and organization's complaints, the FBI detects the data breach and files a report with government affairs.**Typical response**
  - IT security reactively investigates employee data leak, trying to determine the scope of the breach.
  - Team escalates event to privacy team.
- 4 Sensitive data is published on social media**  
Online bloggers publish video with references to the sensitive data stolen.  
**Visible hints**
  - An online video, found by employees, is sent to the head of communications.**Typical response**
  - The security team engages the communications group.

32

**What does a Cyber Security Professional look like?**

**WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?**

**Yo! DUDE... BACK HERE!**

KAL 2008 The Economic

A cartoon illustration featuring a large, heavily armored warrior standing over a smaller figure at a computer. The warrior is holding a massive, multi-barreled gun-like device. A speech bubble from the warrior asks, "WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?". The smaller figure, wearing glasses and a cap, is sitting at a desk with a laptop and a sign that says "CYBER SECURITY", and is shouting, "Yo! DUDE... BACK HERE!". The cartoon is signed "KAL 2008 The Economic".

33

## Multiple Protection for Computers

A data processing system can involve:

- patented hardware and software
- patented computer architecture on circuit designs
- patented business methods
- trade secret production processes
- trade secrecy for collateral know-how
- copyrighted microcode
- copyrighted operating system
- copyrighted instruction manual
- semiconductor chips protected as mask works
- consoles or keyboards protected by design patents
- or as trade dress under trademark principles
- trademark registration

34

## How We Protect Information?

### □ People

- Training, education, awareness, repetition

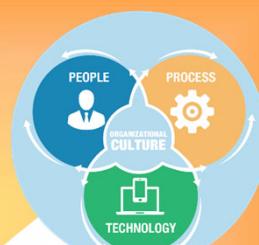
### □ Process

- Governance, oversight, policy, reporting

### □ Technology

- Firewalls, IDS/ISP, SIEM, anti-malware
- Strong passwords, Logging/monitoring

### □ Which is the weakest link?



35

## Opinion

- People
  - Cyberattacks have to do with psychology
  - People do not care
  - People do not understand
  - Bias affect behaviour
  - People make mistakes, go complacent
  - People are not to be trusted

37

37

## Groups at risk

■ Very likely ■ Somewhat likely ■ Not likely

	Employee populations with access	Insider-threat actions they might take			Likely personas involved
		Fraud/theft	Exposure	Destruction	
Top assets					
Intellectual property for new products	• R&D team • Business-unit (BU) exec	■		■	• Flight risk • Disgruntled
Financial forecasts	• Finance/investor-relations team • BU execs	■	■		• Financially stressed • Negligent
PII/PHI <sup>1</sup>	• HR team • Sales team	■		■	• Negligent • Reckless • Snooper
High-net-worth customer information	• High-net-worth sales and delivery team	■		■	• Flight risk • Financially stressed
Core financial platform	• IT team • BU execs	■		■	• Saboteur • Disgruntled
Records of corporate conduct	• HR/legal		■	■	• Attention seeker

<sup>1</sup> PII = personally identifiable information, PHI = protected health information.

38



## Cyber Security and Privacy Starts and Ends with People!

Commit to a disciplined practice of information security and continue to refresh yourself so you don't become a point of vulnerability in our security defenses.

39



## Situational Awareness

- To practice good situational awareness, take the following precautions, including but not limited to:
  - Avoid discussing topics related to business outside premises, whether you are talking face to face or on the phone
  - Remove security badges after leaving your office
  - Don't talk about work outside office
  - Avoid activities that may compromise situational awareness
  - Be discreet when retrieving messages from smart phones or other media



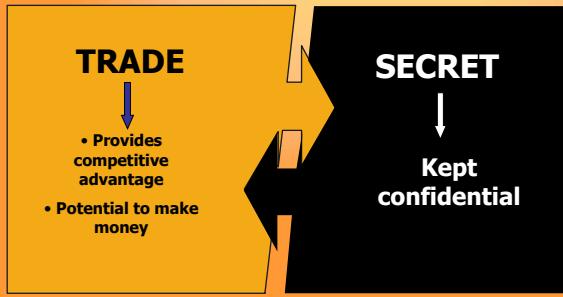
40

40



### General principles:

- Information that has **commercial value** and that has been **scrupulously kept confidential** will be considered a trade secret (TS).
- Owner will be entitled to **court relief** against those who have stolen or divulged it in an illegal manner.



**TRADE**

- Provides competitive advantage
- Potential to make money

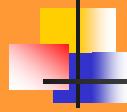
**SECRET**

Kept confidential

41



42



## Legal Action

**COURT RELIEF if:** TS + "THEFT"

Only theft if wrongful !

Courts will only grant relief if someone has **improperly acquired, disclosed or used the information**

43

## Trade-secrete & employees

1. New employees
  - Brief on protection expectations early
  - Obligations towards former employer!
  - Assign all rights to inventions developed in the course of employment
  - NDA/CA
  - Non-compete provision
2. Current employees
  - Prevent inadvertent disclosure (ignorance)
  - Train and educate
  - NDA for particular task
3. Departing employees
  - further limit access to data
  - exit interview
  - letter to new employer
  - treat fairly & compensate reasonably for patent work

•Reqs  
•Limits

44



## Non-Competition Clauses (covenants not to compete) in Labour Contracts

After employee leaves prior employer:

- May he work for competitor?
- May he work in related job?
- May he open a competing business?
- Is covenant not to compete enforceable?

45



### ***Class built slide (2024 and 2025)...***

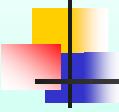
- May he work for competitor?  
Employee: Yes. After: Yes
- May he work in related job?  
Employee: Yes. After: Yes
- May he open a competing business?  
Employee: No. After: Yes
- Is "covenant not to compete" enforceable?  
Yes, by rightful termination with employee.

**Real answer – depends on the LAW and on the legal framework (country, court).**

**For international contracts this is an essential caution for the employee** (note: trade secrets link here)

46

46



## LAWFUL INTERCEPT – THE TECHNOLOGY

48



### Why lawful (legal) Intercept?

- How to fight
  - Terrorism
  - Pedophilia rings
  - Cyber stalking
  - Data theft
  - Industrial espionage
  - Illegal trade (e.g. drugs, guns) on the internet
- What are the problems with Legal Intercept?
  - Privacy
  - Security

49

49



## Two types of LI

- **Passive Interception:** This enables LEAs to capture the delivery of data and voice communications, providing the ability to filter and extract data and voice.
- **Active Interception:** This enables LEAs access to service provider networks by providing standardized interfaces for real-time access to communication service during investigations.

50

50

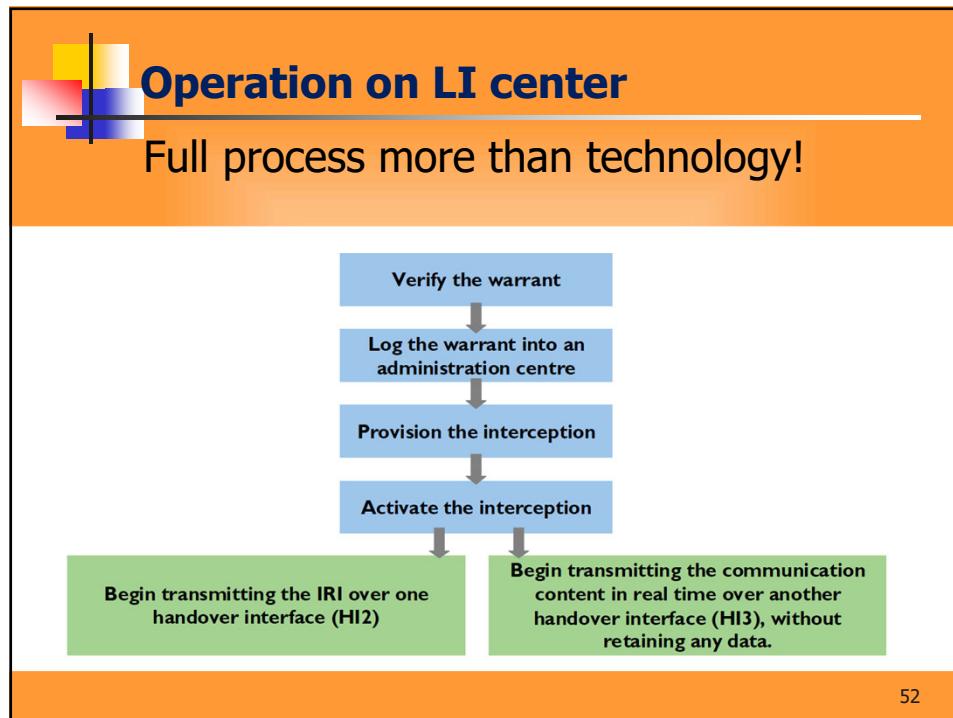


## Two types of information

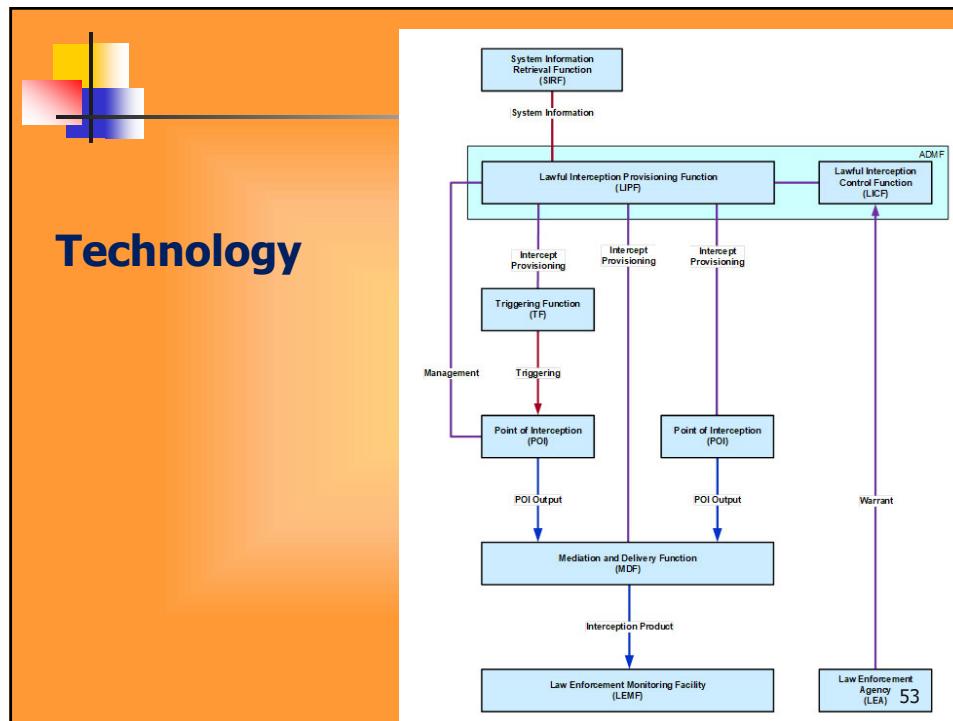
- **Content of communications (CC)** - This refers to the information exchanged between two or more users. This includes voice, video, chats, information or message contents.
- **Intercept Related Information (IRI)** - This is a collection of information or data related to the target. This includes location, log or successful and unsuccessful communication attempt, source and destination of calls, IP addresses, time or duration, Metadata, etc.

51

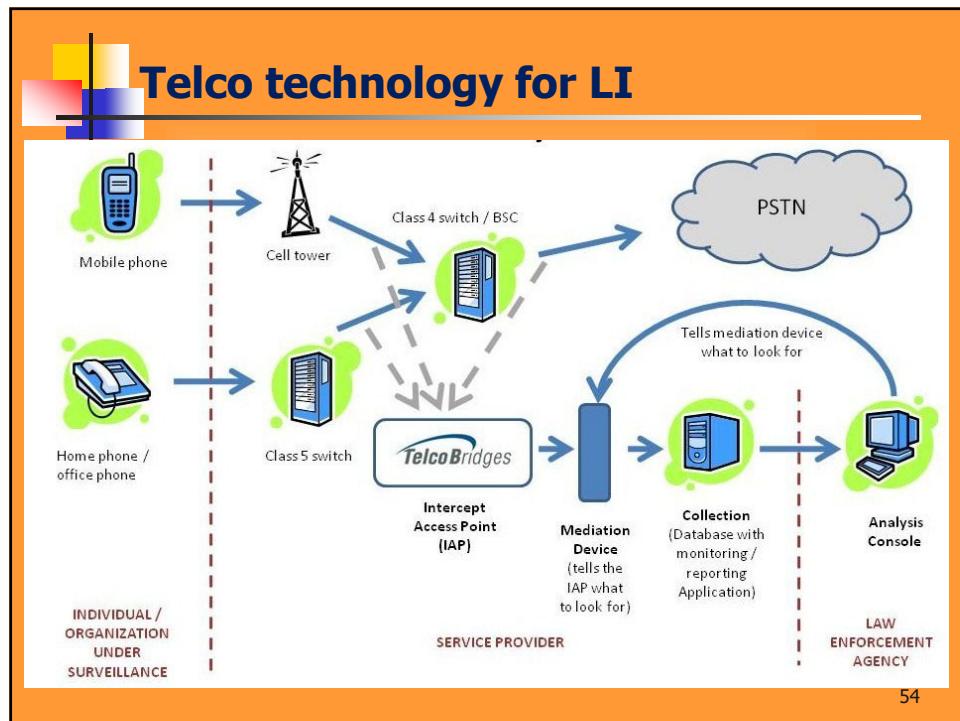
51



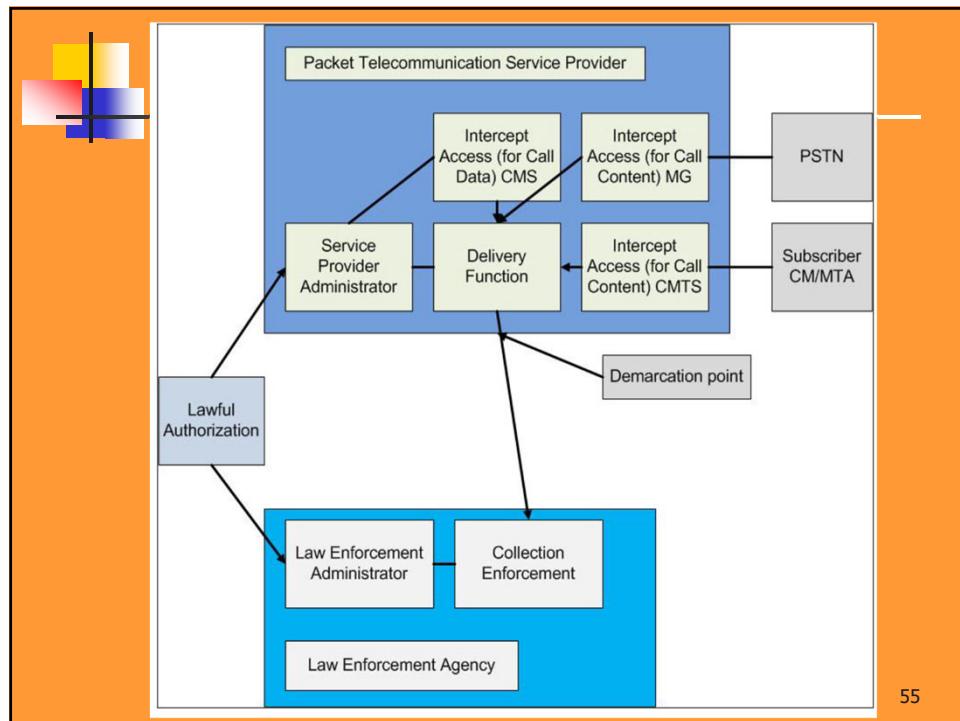
52



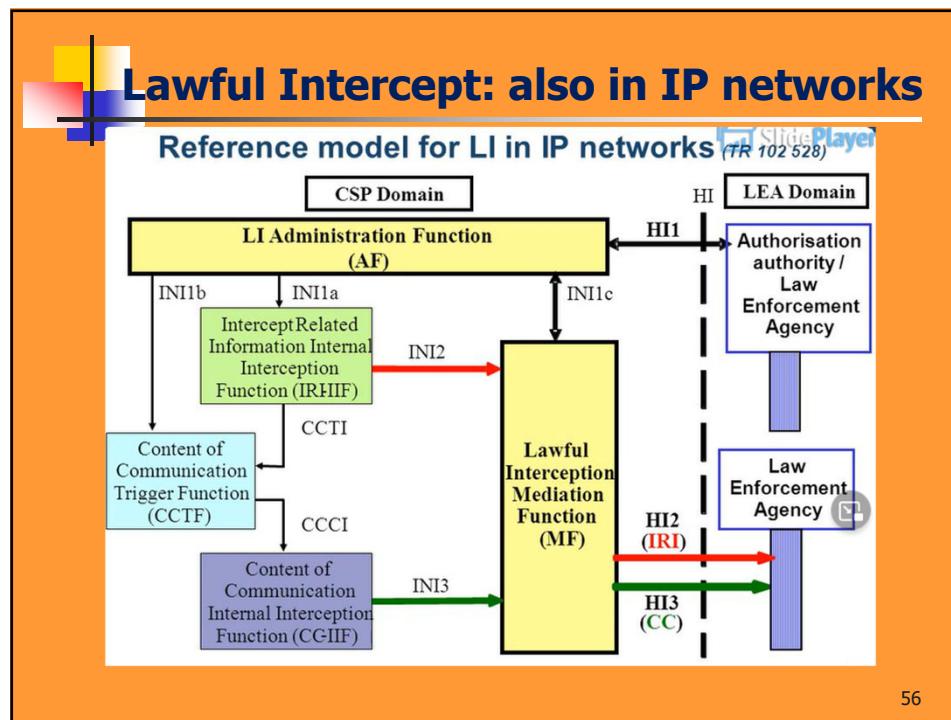
53



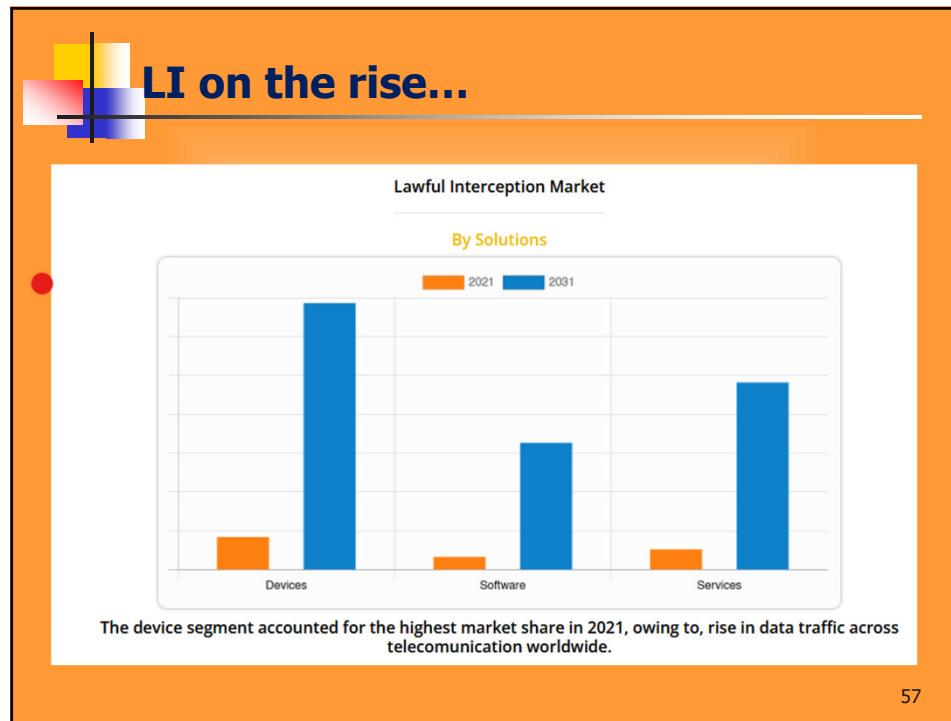
54



55

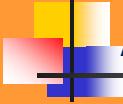


56



57

57



## Admissibility of Surveillance?

- Virtual Locus Delecti (legal concept of proof)
  - Hard to actually find criminals in delicto flagrante
  - How to handle expert evidence?
    - Juries are not composed of network specialists.
    - Legal not scientific decision making.
- Intercepted evidence is often seen as secondary and not primary evidence
  - Primary is the best possible evidence e.g. in the case of a document its original.
  - Secondary is clearly not the primary source e.g. in the case of a document copy.

58

58