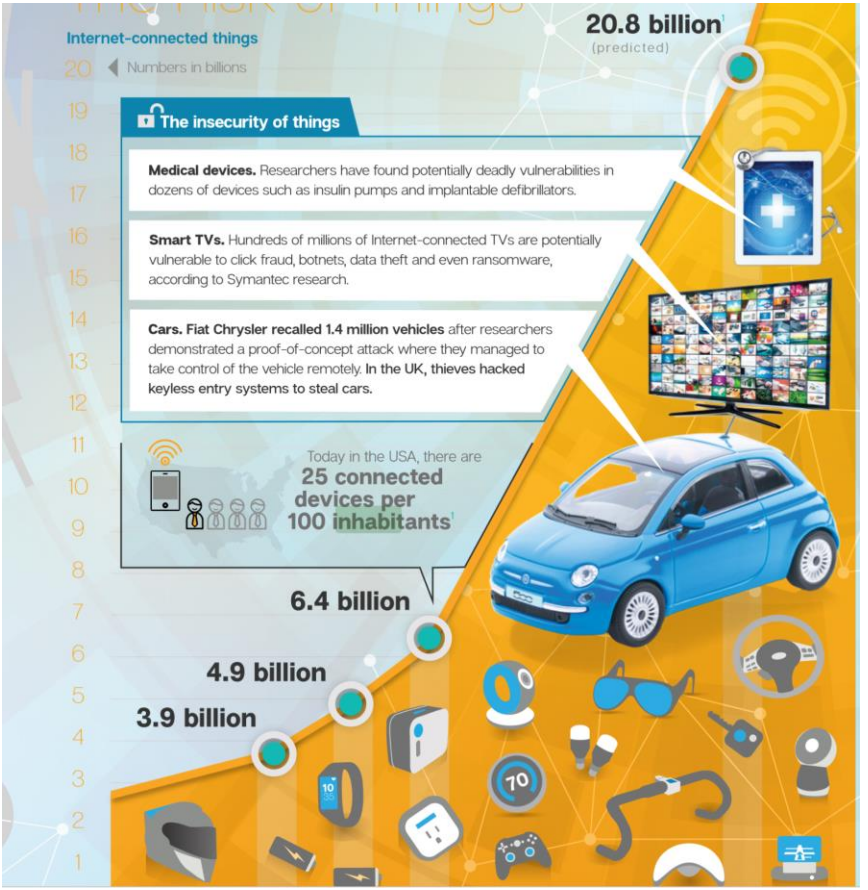
Future threats and roadmap for Europe

Claudio A. Ardagna, Università degli Studi di Milano

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Scenario

- Today environment is rapidly changing
  - Distributed system, Internet computing, Software-Defined Networks, Cloud computing, Edge computing
  - A **huge amount of data** are generated and collected every minute (sensors)
  - 1.7 million billion bytes of data, over 6 megabytes for each human (2016)
  - **2.5 quintillion bytes of data created each day**
- The trend is rapidly accelerating with the **growth of the Internet of Things** (IoT), 200 billions of connected devices by 2020 according to Intel
  - Billions of connected smart devices and sensors
  - "**IoT will account for one-quarter of the global 41 million 5G connections in 2024**." - Machina Research forecasts
- **Low latency access** to huge distributed data sources has become a value proposition
- Business intelligence applications require **proper big data analysis and management functionalities** (Artificial intelligence)



Symantec Internet Security Threat Report

Challenges

"Cybersecurity is the second emergency in Europe, only after the climate changes and before the immigration"

National Institute of Standards and Technology
U.S. Department of Commerce

The ability of an organization to determine cause-and-effect relationship is "one of the largest challenges" affecting measurement of cybersecurity

Cost of **known** attacks

45B$ in 2018

Challenges

- Today distributed and mobile paradigm introduces **new security risks**
  - Users **fully/partially lose control** on their data/applications
- Many users express **little trust** in the **correctness and reliability** of software/services they use
  - Security benchmarks, often coupled with static and manual verification activities, are used to evaluate security
- Users' lack of trust has triggered an **increasing public demand** for improving the security of mission and safety-critical software/services
- A huge **interdisciplinary research effort** has been devoted to finding methods for creating security, safety, and dependability…

… but still we are far from a solution

Feeling of Insecurity

Data Breach

1 out of 4

Housebreaking

1 out of 60

70% of organizations say that they believe their **security risk increased significantly** in (Ponemon Institute's Cost of Data Breach Study)

69% of organizations believe the threats they are seeing **cannot be blocked by their anti-virus software** (Ponemon Institute's Cost of Data Breach Study)

Nearly **half of the security risk** that organizations face **stems from having multiple security vendors and products** (Cisco)

Some Statistics

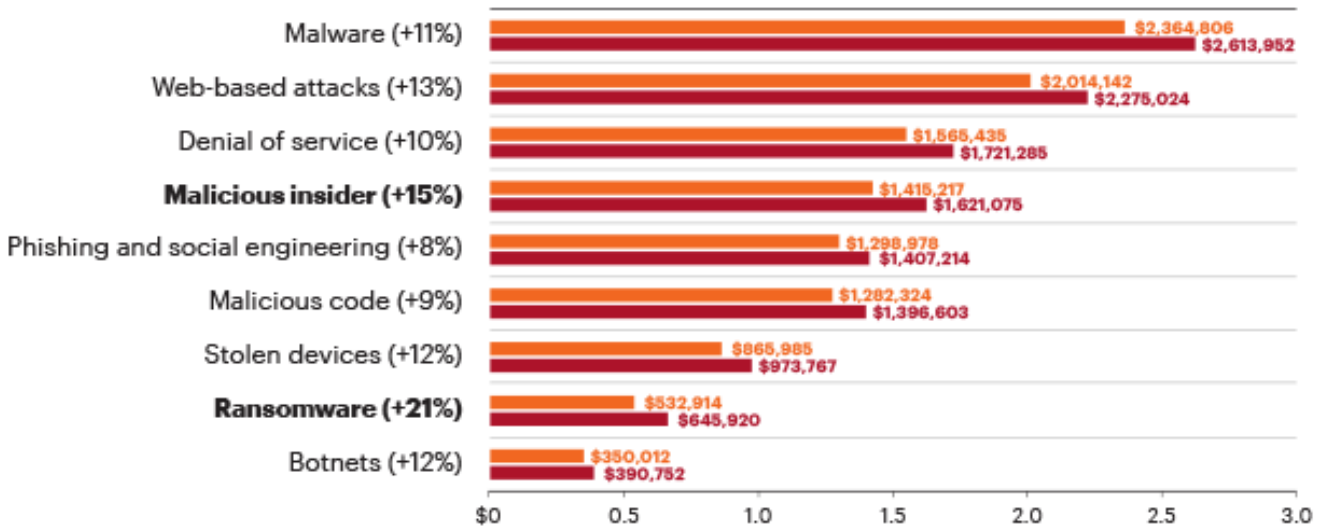
- Big enterprises and national critical infrastructures receive IT attacks **every day**
  - There is a hackers **attack every 39 seconds**
- **43% of cyber attacks** target small business (64% of companies experienced web-based attacks, 62% phishing & social engineering attacks, 59% malicious code and botnets, 51% denial of service attacks)
- Internet of Things (IoT) attacks increased 600% between 2016 and 2017 — Symantec, 2018

Some Statistics

- Since 2013 there are **3,809,448 records stolen** from breaches **every day**, 158,727 per hour, 2,645 per minute and 44 every second of every day
- The **average cost** of a data breach raised to **$3.9 million** (Ponemon Institute's Cost of a Data Breach Report 2019)
  - The U.S. is the most expensive country
  - Healthcare is the most costly industry
  - System glitches and human error breaches are still costly, with an average loss of $3.24 million and $3.5 million
- In 2019, the **average number of breached records** by country was **25,575** (Ponemon Institute's Cost of a Data Breach Report 2019)
  - Cost per lost records is 150$
  - Time to identify and contain a breach is 279 days

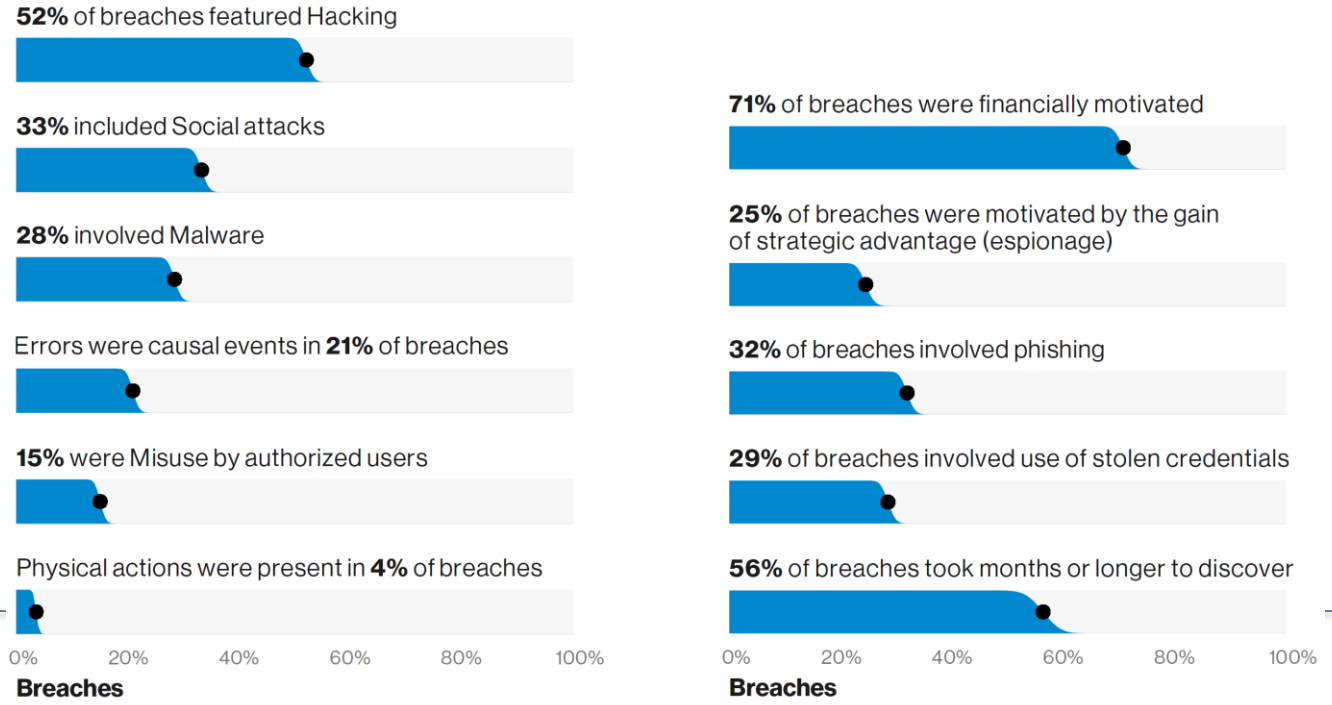
Some Statistics

- Cybersecurity Ventures reportedly estimates that the global cybersecurity space will grow at a CAGR of 9.8% to reach $170.2 billion by 2020. Approximately $1 trillion is expected to be spent globally on cybersecurity by 2021
- Europe faces a projected cybersecurity skills gap of 350,000 workers by 2022, according to a survey by information security certification body (ISC)2
- Only **38% of global organizations** claim they **are prepared** to handle a sophisticated cyberattack

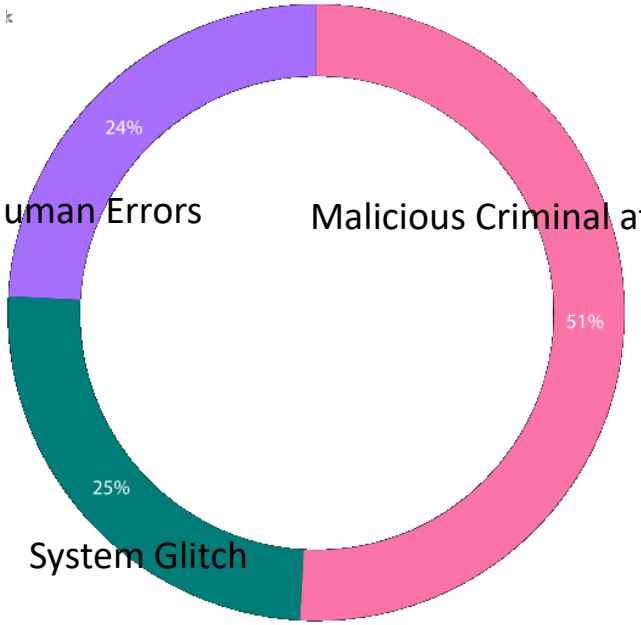


https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

2019 Data Breach Investigations Report - Verizon



Ponemon Institute's 2019 Cost of Data Breach Study



Recent Attacks

theguardian

news / opinion / sport / arts / life

Hospitals

NHS seeks to recover from global cyber-attack as security concerns resurface

Cybersecurity centre says teams 'working round the clock' to fix systems rendered inaccessible by international ransomw

NHS RightCare

verizon

Verizon Confirms Data on 6M Customers Was at Risk

By Donna Fuscaldo | July 13, 2017 — 11:20 AM EDT

A Typo Took Amazon S3 Offline

Amazon Web Services suffered a major outage a few days ago. It turns out one mistyped command is to blame for hours of chaos.

By Matthew Humphries March 3, 2017 6:47AM EST

The Telegraph

HOME | NEWS |

Technology

Technology

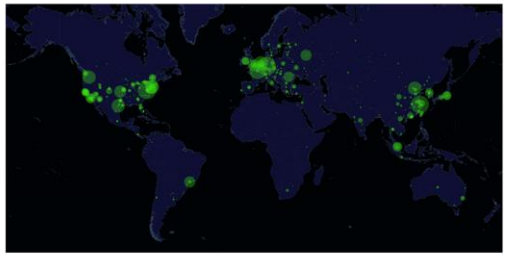
Equifax hackers targeted 15.2 million UK records

Recent Attacks

Ransomware

40K Unprotected MongoDB over internet

January 2015:
"Our initial port scan revealed 39,890 instances. However, this number might be inaccurate, since on the one hand many larger providers blocked the scan such that there might be more publicly accessable MongoDBs online, and on the other hand some of these databases might be intentionally configured without security measures, e.g. as honeypots."



https://cispa.saarland/wp-content/uploads/2015/02/MongoDB_documentation.pdf

The largest DDoS attack launched on service provider Dyn using an IoT botnet

Lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices (digital cameras and DVR players) and then use known default usernames and passwords to log in, infecting them with malware.

- Manage Breaks
- Turn the vehicle
- Unintended acceleration

- One of the reasons was the use of an unsigned firmware

Security researchers Charlie Miller and Chris Valasek

https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/

- Billy Rios reported in 2015 that he'd found vulnerabilities in a popular drug infusion pump that **would allow a hacker to raise the dosage limit on medication delivered to patients**
- More serious vulnerabilities was found in several models of pumps made by the same manufacturer, which would allow a hacker to surreptitiously and remotely change the amount of drugs administered to a patient

- Baby-cams and CCTV hacked.
- "A kid was scared at night because he could hear someone talking to him"

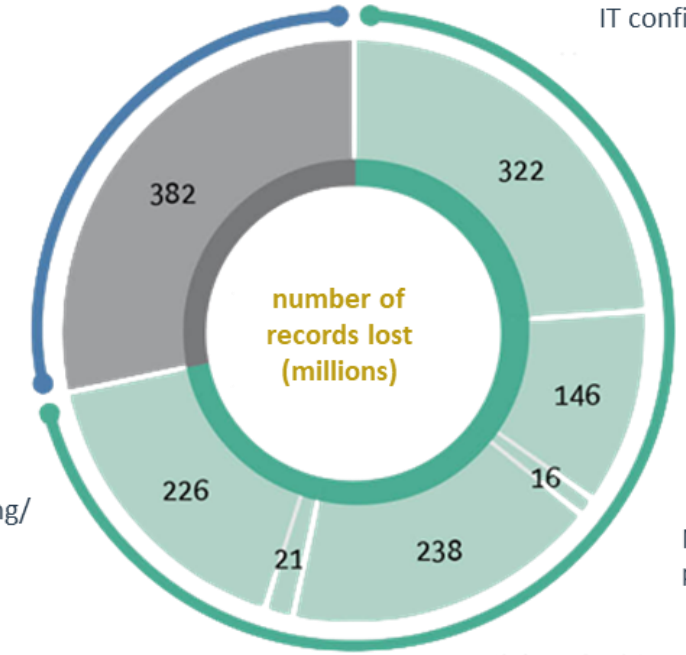
http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/

Other Attacks

- In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time (Oath.com)
- In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers (Uber)
- In 2017, 412 million user accounts were stolen from Friendfinder's sites (LeakedSource)
- In 2017, 147.9 million consumers were affected by the Equifax Breach (Equifax)

Security Breaches & Data Losses

INADEQUATE SECURITY TECNOLOGY
28%



IT configuration errors **23%**

ORGANIZATIONAL, PROCESS, AND PEOPLE FAILURES 72%

Failure to fully implement purchased security product

Negligent insider (accidental publication)

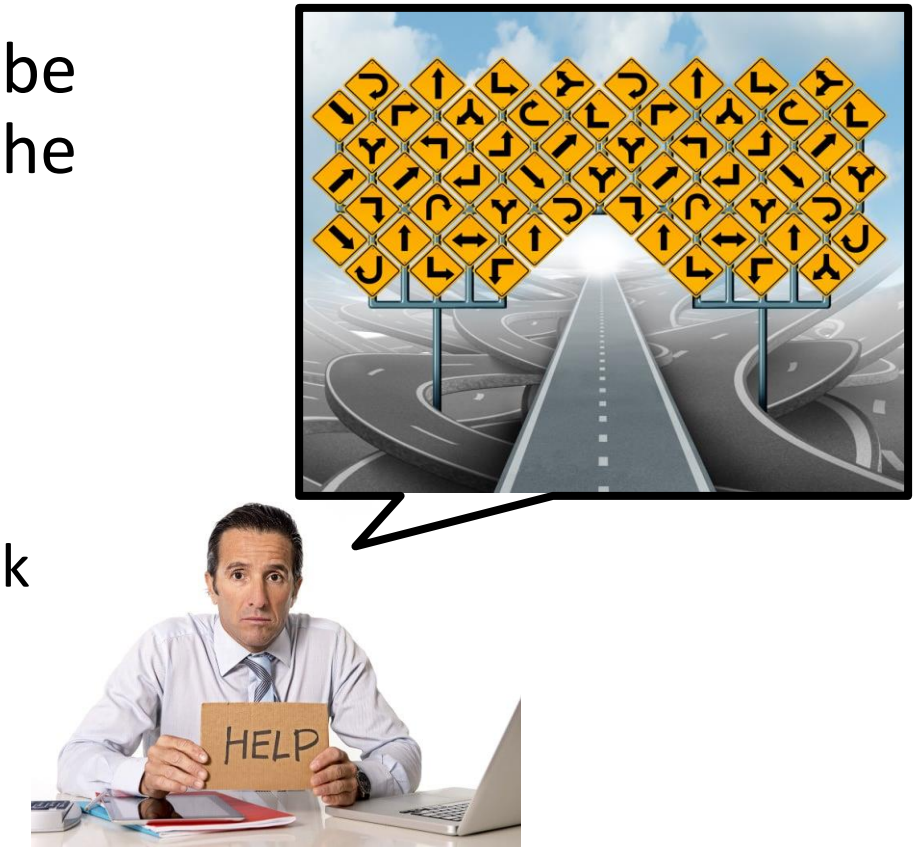
Malicious insiders

Physical loss

Social engineering/ phishing

Security Layers

- Security (across CIA triad) have to be addressed at **different layers** within the system
  - Network access security
  - Network application security
  - Service-layer security
  - Security of data transmitted at different network layers
  - User security

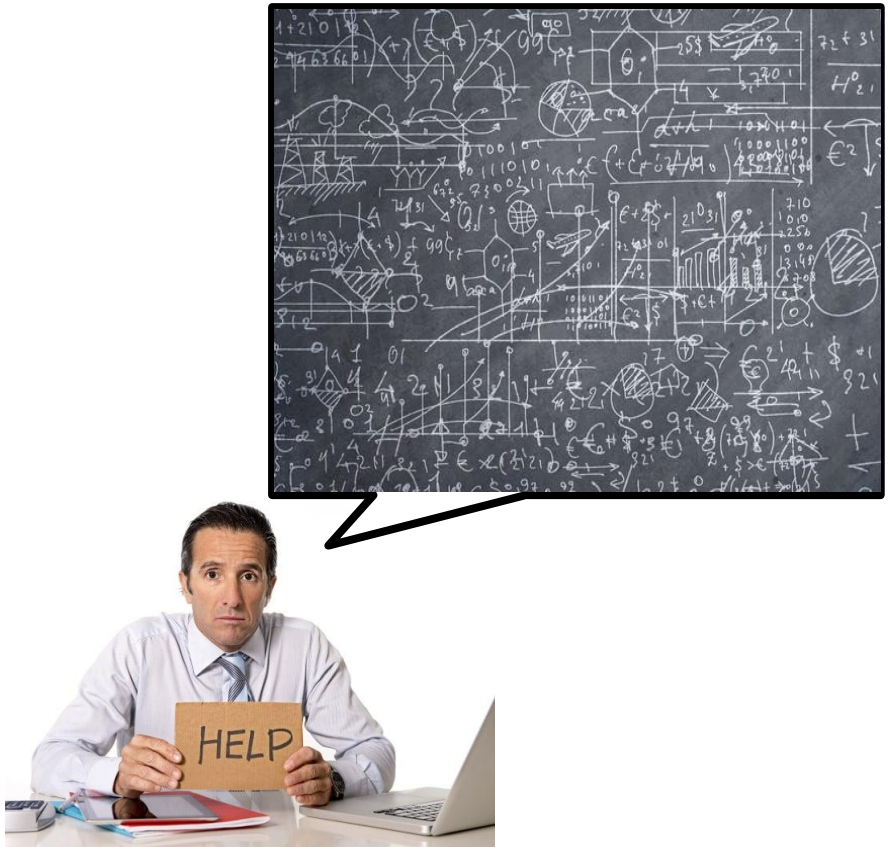


Attack Surface

- **Different and heterogeneous actors and device types** with different requirements
  - Access to billions of potentially **vulnerable** or already **exploitable devices** (e.g., weak/default/shared passwords, unpatched devices, cleartext communications)
- **Lack of guidelines** for connected device management
  - Increased digital footprint that could expose personal or sensitive data
- **Untrusted providers**
- **Fuzzy perimeters**
- **Untrusted collected data**

Gaps

- Lack of appropriate **compliance and certification standards**, making analysis, detection and reporting complicated
- Lack of **continuous assurance and compliance assessment**
- Lack of **trustworthy evidence** coming from untrusted devices
- Attacks evolve **more rapidly** than corresponding security solutions



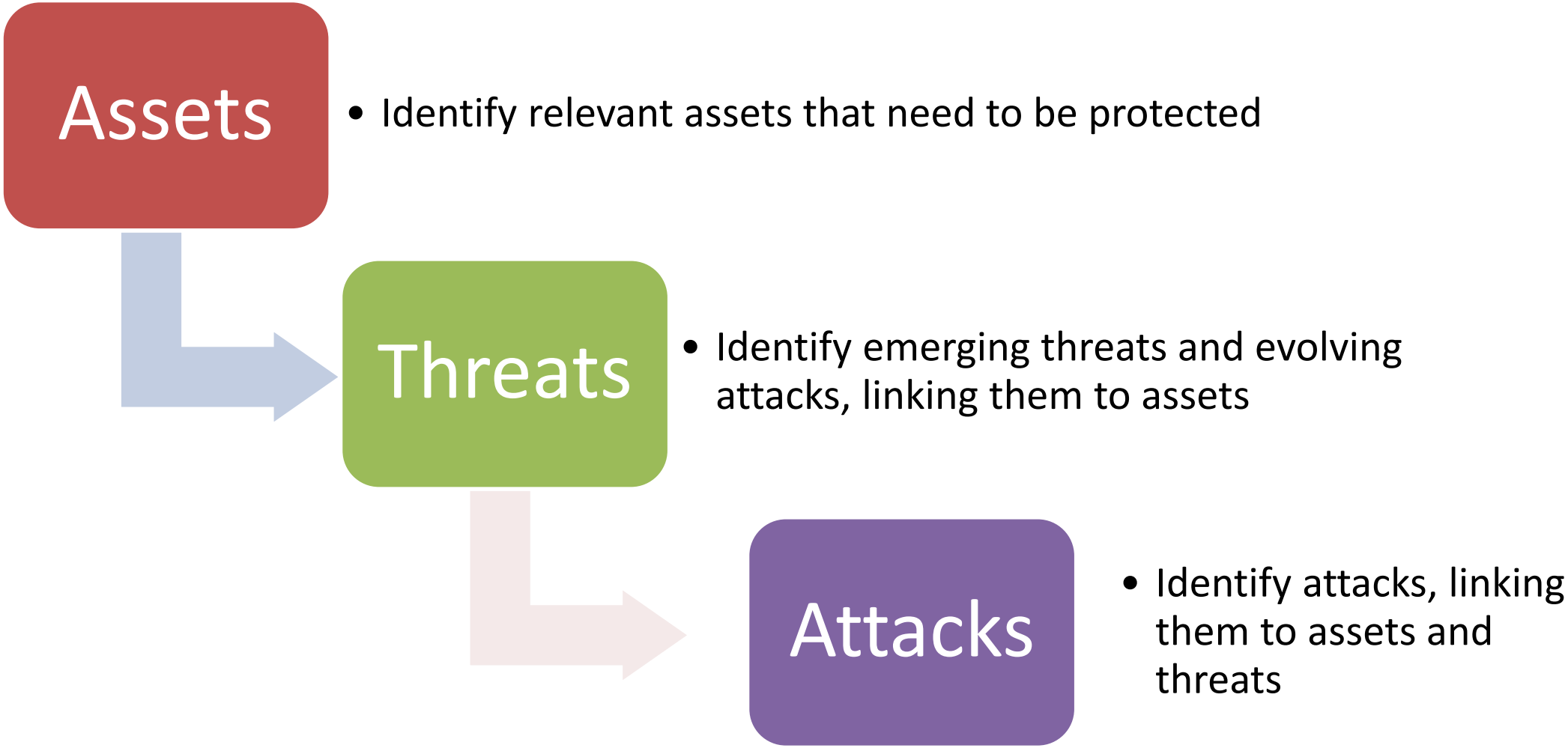
Requirements

- **Multitude of security requirements**
  - Manage security procedures in scenarios asking for **extremely low latency**
  - Security and privacy across **multiple networks, multiple parties** or **shared infrastructures**
  - Data security (**CIA triad**) for low complexity, low throughput services and sensors
  - Protect customer identity, location and privacy
  - **Data verifiability** and **trustworthiness**

Threat Landscape and roadmap

- **Identify future and emerging threats** in 5 domains: (i) network-centric, (ii) system-centric, (iii) application-centric, (iv) data-centric, and (v) user-centric security
  - **Current State-of-the-Art** in the area that is addressed by the working group
  - **Outlook of emerging threats and evolving attacks** that can be expected in the future
  - **Gaps and challenges**
  - **Research actions and countermeasures** that need to be taken to mitigate the identified threats

Methodology



Assets

- Data-Centric Security
  - Data, Infrastructure, Big Data Analytics, Security and Privacy techniques, Roles
- Application-Centric Security
  - Data, Interfaces, Security and Privacy techniques, Roles
- System-Centric Security
  - Data, Infrastructure, Middleware, Devices, Management, Security mechanisms, Roles
- Network-Centric Security
  - Core Network, Access Network, Infrastructure Network/Area network, Peering points, Subscriber Assets' Network
- User-Centric Security
  - Data, Privacy techniques, Human, Roles

Data-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors* *Threat T2: Inadequate design and planning or incorrect adaptation*
TG2 – Interception and illegal acquisition	*Threat T3: Interception of information* *Threat T4: Illegal acquisition of information (data breach)*
TG3 – Poisoning	*Threat T5: Data Poisoning* *Threat T6: Model Poisoning*
TG4 – Nefarious Activity/Abuse	*Threat T7: Identity fraud* *Threat T8: Denial of service* *Threat T9: Malicious code / software / activity* *Threat T10: Generation and use of rogue certificates* *Threat T11: Misuse of assurance tools* *Threat T12: Failures of business process* *Threat T13: Code Execution and Injection (unsecure APIs)*
TG5 – Legal	*Threat T14: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG6 – Organisational threats	*Threat T15: Skill shortage* *Threat T16: Malicious Insider*

Data-Centric Security: Current Trends

- **Data breaches and leaks are increasing**
- **Traditional attacks** like phishing and DDoS **are reviving a new boost** and mainly target the confidentiality, integrity, and availability of data
- **Human errors**, as well as **glitches in system configuration**, are still at the forefront of the issues and **facilitate attacks**
  - Lack of skills and competences
  - Increase in system and platform complexity
- **Target phishing and malwares are spreading**
  - Phishing attacks target rich individuals, people with access to financial accounts or sensitive business data or even public authorities that handle PII related data.
  - Malwares target data and in particular wipe, modify, access data with no authorization (30% of all data breaches incidents).

Data-Centric Security: Current Trends

- **EU General Data Protection Regulation (GDPR)** changed the fundamentals of data protection worldwide
  - **New legal requirements** of reporting data breaches
  - **Data breach or leakage can become a new weapon in the cyber criminal hands** (extortion attacks with the threat of GDPR penalties deriving from data disclosure).
- New threats and attacks
  - **Impair algorithm and infrastructure behavior** at the basis of artificial intelligence and machine learning become new targets
  - **Data poisoning** as a huge driver towards more complex attacks
  - **Model poisoning** to fake the learning algorithm in considering a malicious behavior as a normal one

Application-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Security Misconfiguration*
TG2 – Interception and illegal acquisition	*Threat T2: Interception of information* *Threat T3: Sensitive data exposure*
TG3 – Nefarious Activity/Abuse	*Threat T4: Broken Authentication and Access Control* *Threat T5: Denial of service* *Threat T6: Code Execution and Injection (unsecure APIs)* *Threat T7: Insufficient logging and monitoring* *Threat T8: Untrusted composition*
TG4 – Legal	*Threat T9: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG5 – Organisational threats	*Threat T10: Malicious Insider*

Application-Centric Security: Current Trends

- As applications are spreading at all layers of an ICT systems, attacks targeting them are spreading as well
- **Malware attacks continue to rule the roost**, particularly targeting cloud and IoT applications
  - Ransomware are still strong
  - Mobile malware is growing exponentially since 2017 (e.g., mobile banking)
  - DDoS are evolving targeting mobile devices and sensors, and mainly battery consumption
- The increase in **platform complexity** and the proliferation of many (third-party) libraries **open the door to new attacks** (e.g., privilege escalation, hijacking, code execution) that threaten not only the platform itself, but also the users relying on it

Application-Centric Security: Current Trends

- **Single and not-expert users are directly involved in complex business processes**
  - Configuration errors are therefore increasing as never seen before
    - E.g., wrong access policies, weak passwords, unpatched systems, and the like, make the overall environment unsecure
  - Personal data of the users can be stolen and sold on the black market
  - Entire systems can be hijacked and remotely controlled, while specific sensors/devices put offline by exhausting their resources
- **Micro-service architecture** has increased the revenue for enterprise and supported new businesses, while **neglecting non-functional properties** such as security and privacy

System-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors* *Threat T2: Inadequate design and planning or incorrect adaptation*
TG2 – Interception and illegal acquisition	*Threat T3: Interception of information*
TG3 – Poisoning	*Threat T4: Configuration/data Poisoning* *Threat T5: Business process/orchestration Poisoning*
TG4 – Nefarious Activity/Abuse	*Threat T6: Identity fraud* *Threat T7: Denial of service* *Threat T8: Management Hijacking* *Threat T9: Misuse of assurance tools*
TG5 – Organisational threats	*Threat T10: Malicious Insider*

System-Centric Security: Current Trends

- Current systems are based on a **number of software layers** and in most of the cases including virtualization layer
  - The security of multi-layer systems is the security of the weakest layer
  - Increasing sharing level and multitenancy exacerbate the impact of most of the threats
  - They inherit and make the weaknesses of traditional systems worse
- **IoT enlarges the perimeter of the system** including devices with very basic capacities in terms of security features due to cost constraints
  - Security features are insufficient compared to the emerging threats
  - Physical access to IoT device will be exploited more in the future as bridge to generate threats based on malicious insiders

Network-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Erroneous use or administration of devices and systems*
TG2 – Interception and illegal acquisition	*Threat T2: Interception of information/Man in the middle* *Threat T3: Interception/man-in-the-middle* *Threat T4: Interception of information/Man in the middle* *Threat T5: interception/man in the middle traffic redirection*
TG3 – Nefarious Activity/Abuse	*Threat T6: Exploitation of software bug* *Threat T7: Manipulation of hardware and firmware* *Threat T8: Malware and virus- Saturation attacks* *Threat T9: Remote activities (execution)*
TG5 – Legal	*Threat T10: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG6 – Organisational threats	*Threat T11: Failures of devices or systems* *Threat T12: supply chain* Threat T13: software bug

Network-Centric Security: Current Trends

- Network environments are **more and more dynamic**, expanding the network perimeters and requiring multiple layers of defence to mitigate vulnerabilities
- **Everything connected to a network becomes a target**
  - Attack surfaces include traditional servers, as well as IoT devices and network assets in all 5 domains
- Criminals have **more entry points** than ever before
- New emerging risk factors and threats exploiting the adoption of new network technologies such as 5G, Network Functions, Resource Exhaustion, and many others
- Mobile malware and attacks

User-Centric Security: Threats

Threat Groups	Threats
TG1 – Unintentional damage / loss of information or IT assets	*Threat T1: Information leakage/sharing due to human errors*
TG2 – Interception and illegal acquisition	*Threat T2: Interception of information* *Threat T3: Illegal acquisition of information (privacy breach)*
TG3 – Nefarious Activity/Abuse	*Threat T4: Identity fraud/Impersonation* *Threat T5: Deep Fake* *Threat T6: Reputation Attacks* *Threat T7: Malicious code / software / activity*
TG4 – Legal	*Threat T8: Violation of laws or regulations / Breach of legislation / Abuse of personal data*
TG5 – Human threats	*Threat T9: Skill shortage* *Threat T10: Impersonation/Fake accounts*

User-Centric Security: Current Trends

- With the advent of IoT, **users become just another component of complex systems**
  - Their involvement is increasingly pervasive
  - Complex systems/applications based on data sensed by users devices
  - The trustworthiness of data become fundamental
- **Users become target of attacks**
  - Fake news, fake social accounts, and deep fake to manipulate and altering perception of reality
  - Reputation attacks targeting the reputation of the users through impersonation/fake news
  - Attacks to smart devices and smart homes, making users source of untrustworthy data

Concluding Remarks

- **Cyber attacks increasingly target users and data**
  - Data breaches and leakages provide **increasing revenue for attackers**
  - Users are often sources of attacks (lacks of skills and competences)
- Traditional attacks (e.g., malware, DDoS, social engineering) are experiencing a new boost
  - Attacks attempt to breach those targets (users, components, machines) that could provide much revenue
  - Ransomware retains its dominance, DDoS is a plague, social engineering is still critical, cryptocurrencies abuse is emerging
- **Mobile malware and attacks** are rapidly growing
- **GDPR extorsion and reputation attacks** are on the rise

Concluding Remarks

- **EU Cybersecurity Act**
  - **New mandate for ENISA**
    - EU agency for cybersecurity with permanent mandate, increased responsibilities and resources
    - Setting up and maintain EU cybersecurity certification framework
    - Operational cooperation at EU level for management of cyber incidents and large-scale attacks and crises
  - **European Cybersecurity Certification Framework**
    - Governance and rules for EU-wide certification of ICT products, processes, services
    - Multiple schemes for different domains

Concluding Remarks

- **Security assurance solutions** (audit, certification, compliance) defined to **increase trust and confidence** in the IT systems
  - Provide **transparency** on the behavior of security mechanisms
  - Are based on **trustworthy evidence** that IT systems and providers **behave as expected**
  - Need to guarantee **acceptable and verifiable QoS**
  - Need to **continuously** guarantee security features over the whole IT supply chain

Next Steps

- Evaluate the **new trends in cybersecurity** including emerging threats and evolving attacks
  - E.g., cryptolocker as a new type of attack for reputation downgrade
  - E.g., phishing attacks that target smart devices (e.g., Amazon ALEXIA)
- Build a **shared knowledge on emerging threats and evolving attacks**, which possibly evolves over time
  - New relations between assets/threats/vulnerabilities (similar to, evolution of, analogy…)
  - The basis for AI-based cybersecurity (e.g., retrieve all evolutions of a particular threat for a particular domain/device)
  - Infer new possible paths of evolution
- Contribute to the CONCORDIA cybersecurity roadmap for EU
  - Providing guidance and setting concrete priorities for policy makers and relevant stakeholders

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.instagram.com/concordiah2020.eu