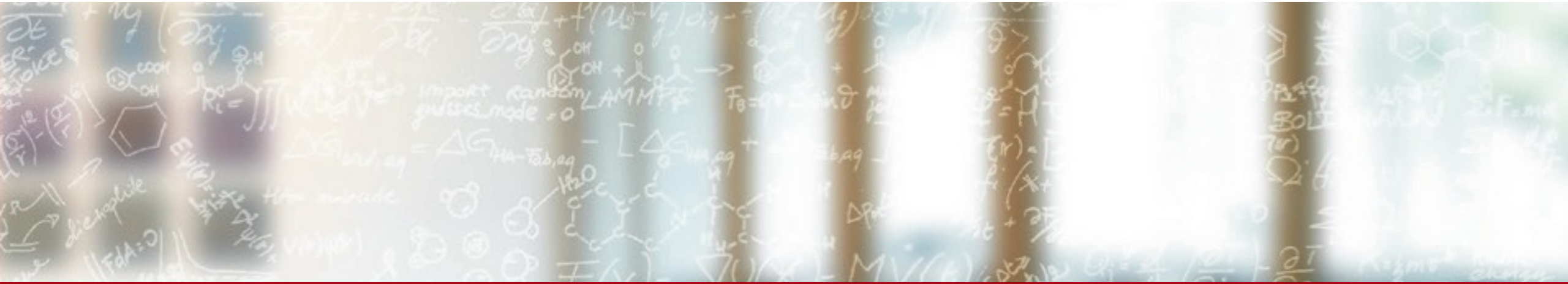




**CSCS**

Centro Svizzero di Calcolo Scientifico  
Swiss National Supercomputing Centre

**ETH**zürich



# Security Matters

HPC-CH

17 May 2018

# Management and Security of Sensitive HPC Data

- Standards & Regulations

- NIST / DoDAF / PCI-DSS
- HIPAA / HITECH / GDPR

- „HPC“ Data

- Volume / Performance / Openness

# Threat Landscape

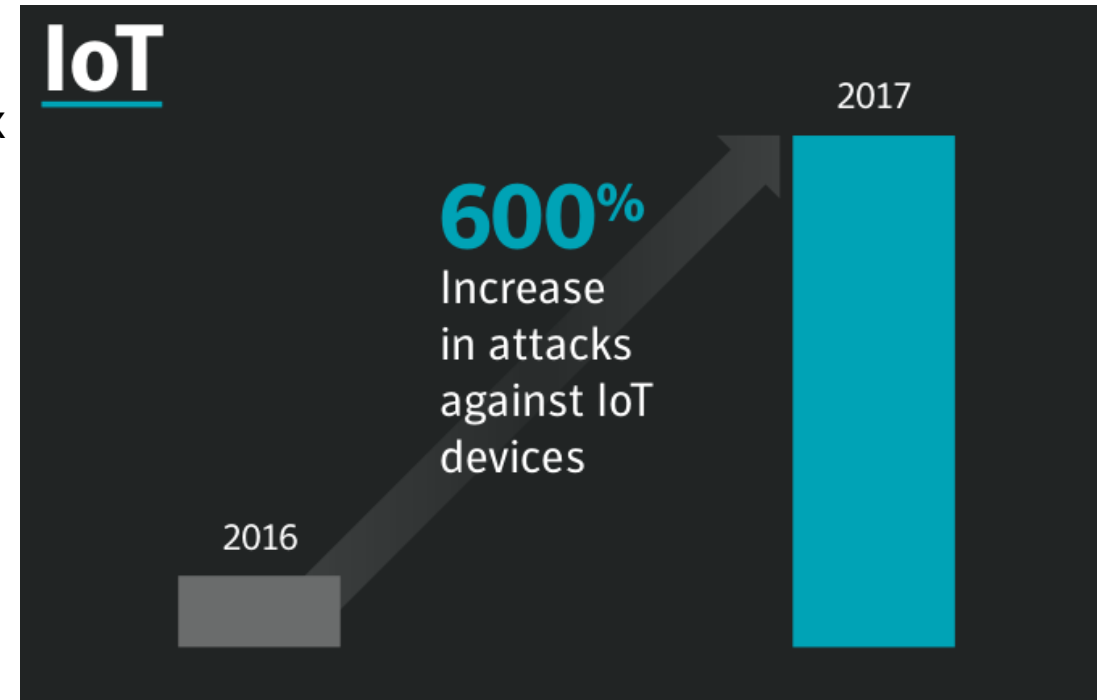
- Traditional HPC: Research Institutes / Military
- Shared by people from multiple entities
- Distributed data sources
- Heterogenous cluster

# Until the threat shifted from the Finance to the Healthcare sector

- What is more valuable:
  - Credit cards or Social security number?
- Finance sector invested a lot on:
  - Security awareness / threat hunting / fraud detection
- Healthcare is far far behind
- Attacks are mostly money driven (Phishing, DDoS, Ransomware)
- Attacks focus on the weakest target with maximum value

# Why is healthcare more profitable for attackers

- The myth of the insurance premium
- Monetization is more reliable
  - Stolen info stays valid a long time
  - People do not easily notice impersonation
  - Fraud investigation (and regulation) is more complex
- Security is not mature
  - IoT / Medical devices
  - Outdated or unsupported systems

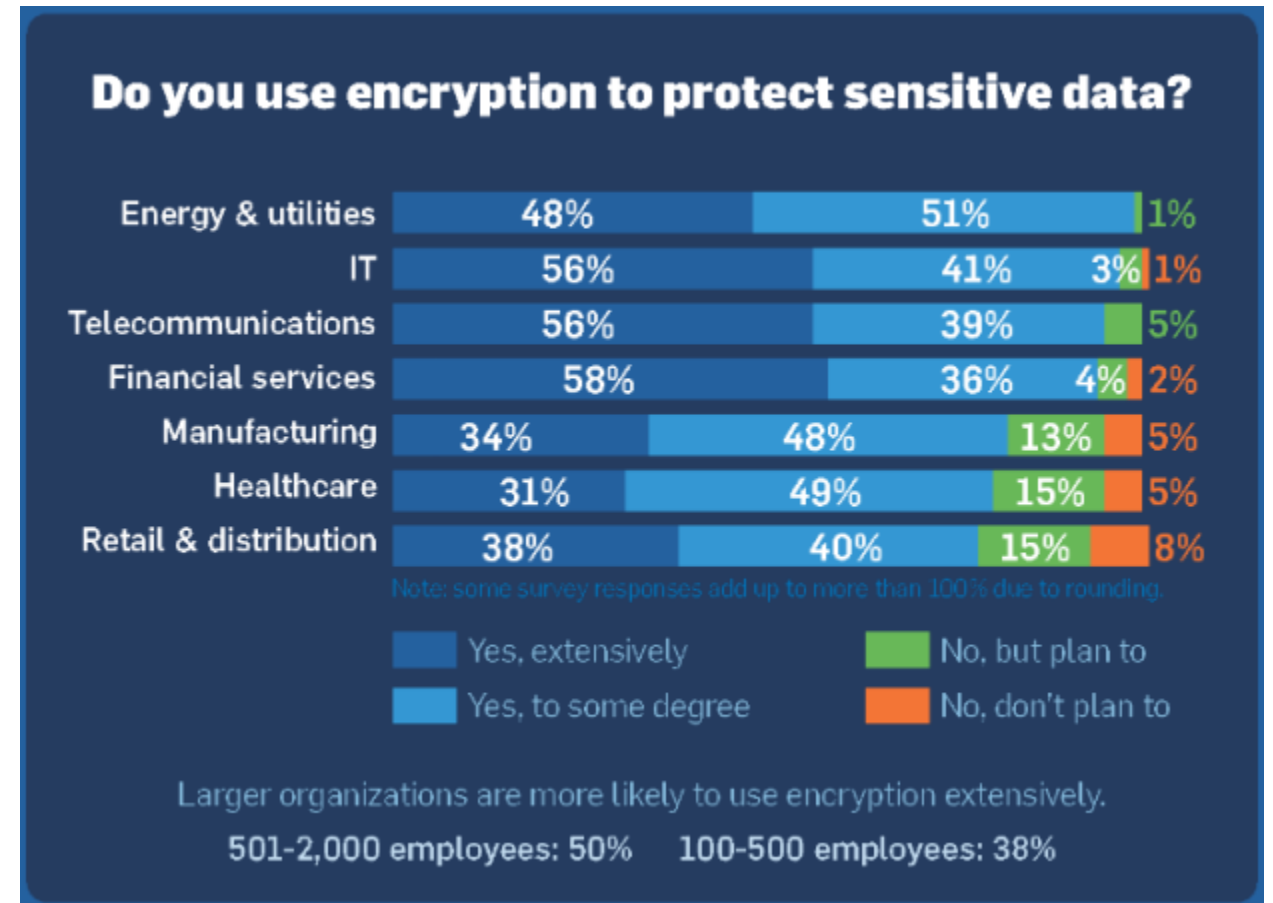


# Sensitive data

- Personally identifiable information
- Risk of discrimination: (sexual orientation, religion, judicial record...)

- Recommendations:

- Make backups
- Rely on encryption
- Keep systems up to date



# Hospital & ransomware

- Weak medical devices
- „Experts say old machines and outdated software at hospitals contributed to the spread of the ransomware, and that could put patient safety further in jeopardy if the situation isn't remedied.“

## [US hospital pays \\$55,000 to hackers after ransomware attack | ZDNet](https://www.zdnet.com/.../us-hospital-pays-55000-to-ransomware-...)

<https://www.zdnet.com/.../us-hospital-pays-55000-to-ransomware-...> ▼ Traduire cette page  
17 janv. 2018 - The **hospital**, based in Greenfield, Ind., revealed that a successful **ransomware** attack on Thursday held the **hospital's** IT systems hostage, ...

## [Indiana hospital shuts down systems after ransomware attack ...](https://www.cyberscoop.com/hancock-hospital-ransomware/)

<https://www.cyberscoop.com/hancock-hospital-ransomware/> ▼ Traduire cette page  
15 janv. 2018 - An Indiana **hospital** suffered the first **ransomware** attack aimed at a health care provider this year when part of Hancock Regional **Hospital's** ...

## [U.S. hospitals have been hit by the global ransomware attack - Recode](https://www.recode.net/.../global-eu-cyber-attack-us-hackers-nsa-h...)

<https://www.recode.net/.../global-eu-cyber-attack-us-hackers-nsa-h...> ▼ Traduire cette page  
27 juin 2017 - Major corporations across the world have been hit by a wave of **ransomware** attacks that encrypt computers and then demand that users pay ...

## [WannaCry and Hollywood hospital ransomware attacks crossed a line ...](https://www.scmagazine.com/...hospital-ransomware.../690110/)

<https://www.scmagazine.com/...hospital-ransomware.../690110/> ▼ Traduire cette page  
20 sept. 2017 - The **ransomware** infection that disrupted Hollywood Presbyterian Medical Center in 2016 and the worldwide WannaCry attacks in 2017 caused ...

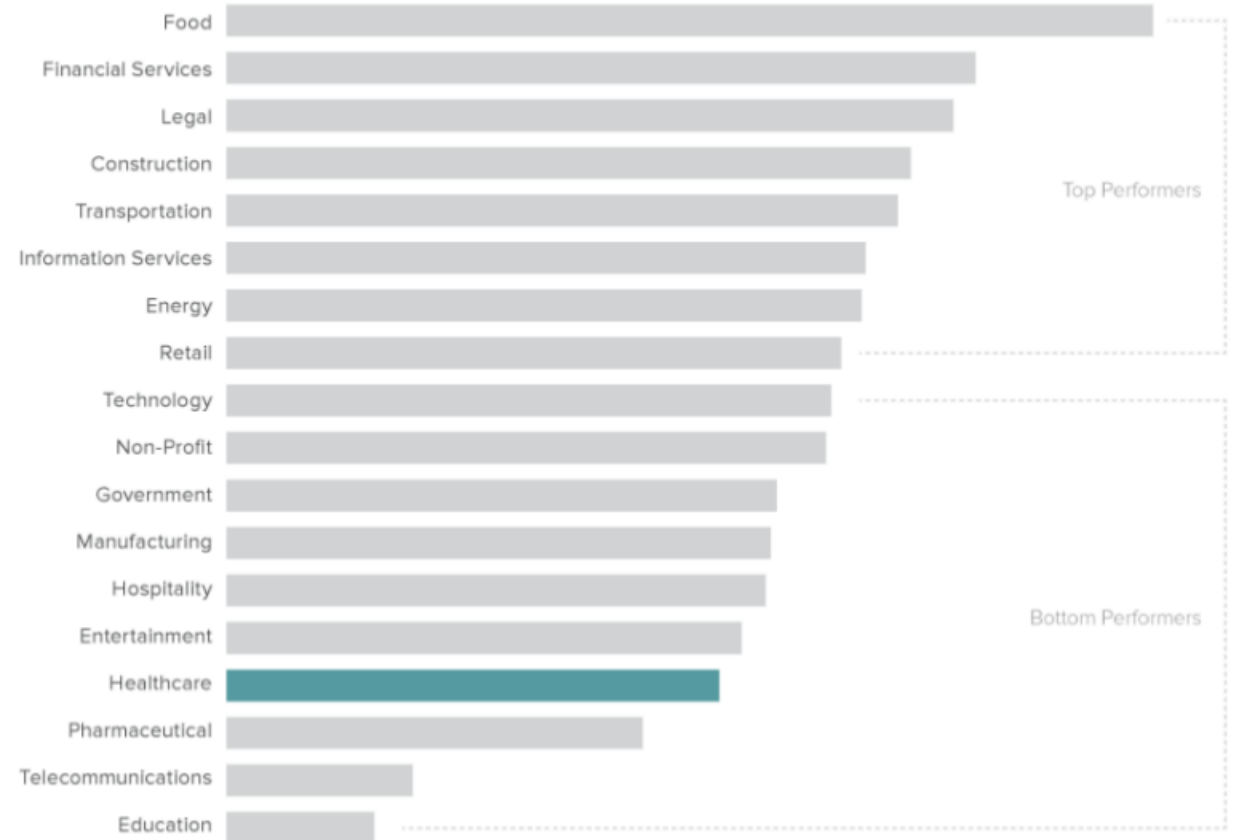
## [Why hospitals are so vulnerable to ransomware attacks - CNN Money](http://money.cnn.com/2017/05/16/.../hospitals...ransomware/index.html)

[money.cnn.com/2017/05/16/.../hospitals...ransomware/index.html](http://money.cnn.com/2017/05/16/.../hospitals...ransomware/index.html) ▼ Traduire cette page  
16 mai 2017 - Bad security at **hospitals** contributed to the **ransomware** outbreak.

# Threat Landscape: Focus on health data

- Traditional researches:
  - Weather and climate
  - Bioscience
  - Physics
  
- Health data, the new gold
  - BigData / Machine Learning
  - Opportunity or threat?

## How the Healthcare Industry Measures up – or Doesn't?





# What can we do?

- Anonymization / de-identification
  - Not always applicable, biometric data, DNA
  - BigData relies on correlation of as much data as possible
  
- Everything we do ends up in a database
  - Facebook, Instagram, SnapChat, Twitter, LinkedIn, Uber
  - All of them reported at least one data breach or information leak
  - False feeling of anonymity / web-tracking
  - Not only „on-line“: Fidelity cards, device-tracking, number-plate recognition, facial recognition...

# What else can we do?

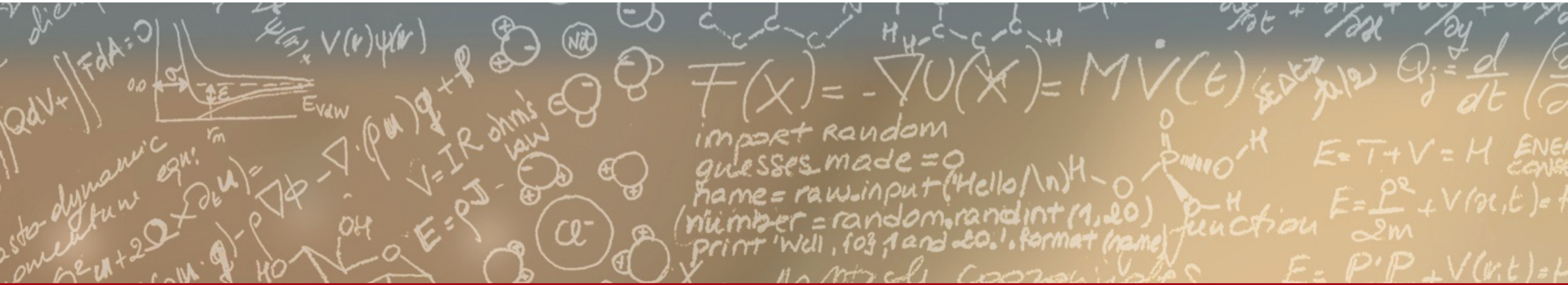
- Follow the security guidelines
  - Even though it will take time to reach a good maturity level
  
- Security awareness
  - Raise concern among professionals
  - Educate the end-users



CSCS

Centro Svizzero di Calcolo Scientifico  
Swiss National Supercomputing Centre

ETH zürich



**Thank you for your attention.**

# References

- Intro to HPC [HPC Advisory Council]
- Where Security Meets High Performance Computing [hpcwire - EMC]
- State of Encryption [Sophos]
- Phishing and Threat Intelligence Report 2017 [PhishLabs]
- Medical record is worth more to hackers than your credit card [Reuters 2004]
- Why Data Security is The Biggest Concern of Health Care [UIC]
- Why cybercriminals attack healthcare more than any other industry [Sophos]
- IT threat evolution Q1 2018 - Securelist [Kaspersky]
- The Value of Stolen Data on the Dark Web [Dark Web News]
- The Rise of Medical Identity Theft [Consumer Reports]