Cyber Security Infrastructure & Its protection

By Muataz Elsadig

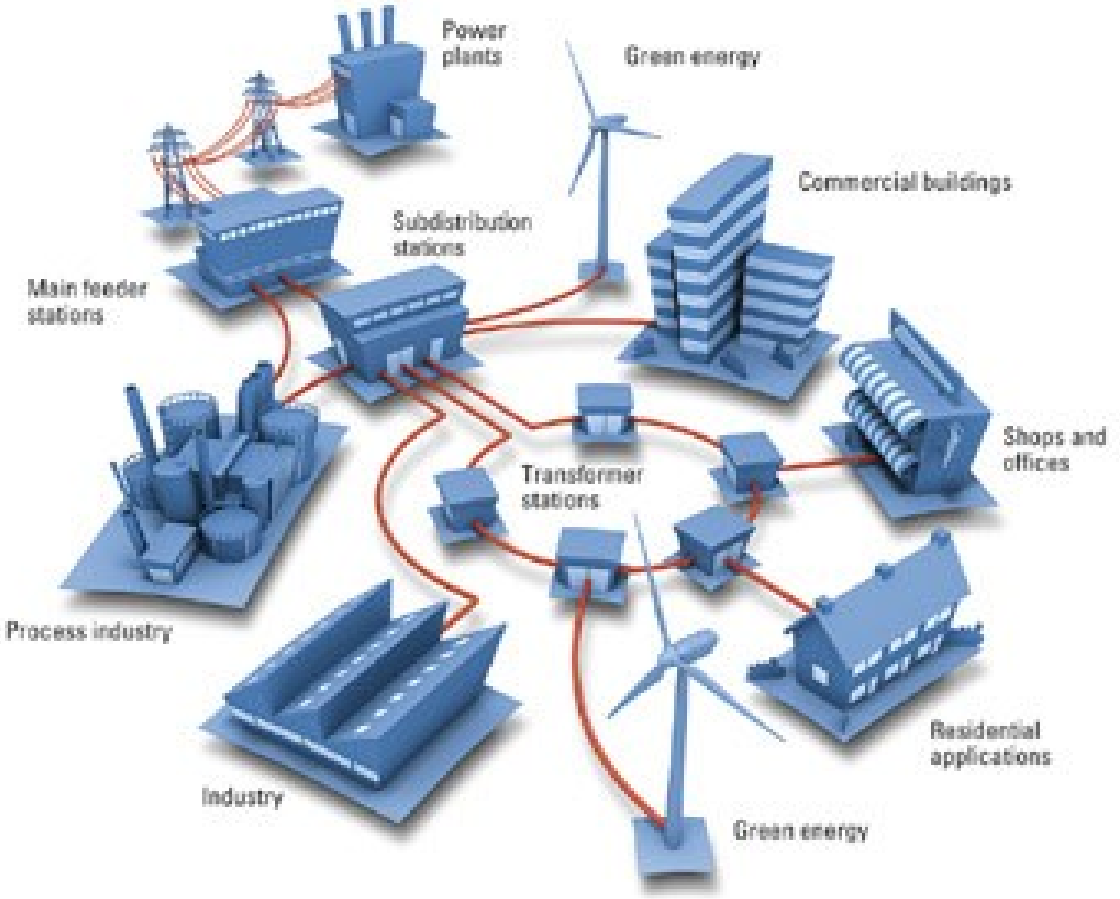
Regional Development Forum for the Arab States,
Khartoum, Republic of Sudan 29 January,2017

Industrial Control System Are Interconnected

Internet

- **2.2 million internet connected devices from 182 manufacturers discovered (Project Shine)**

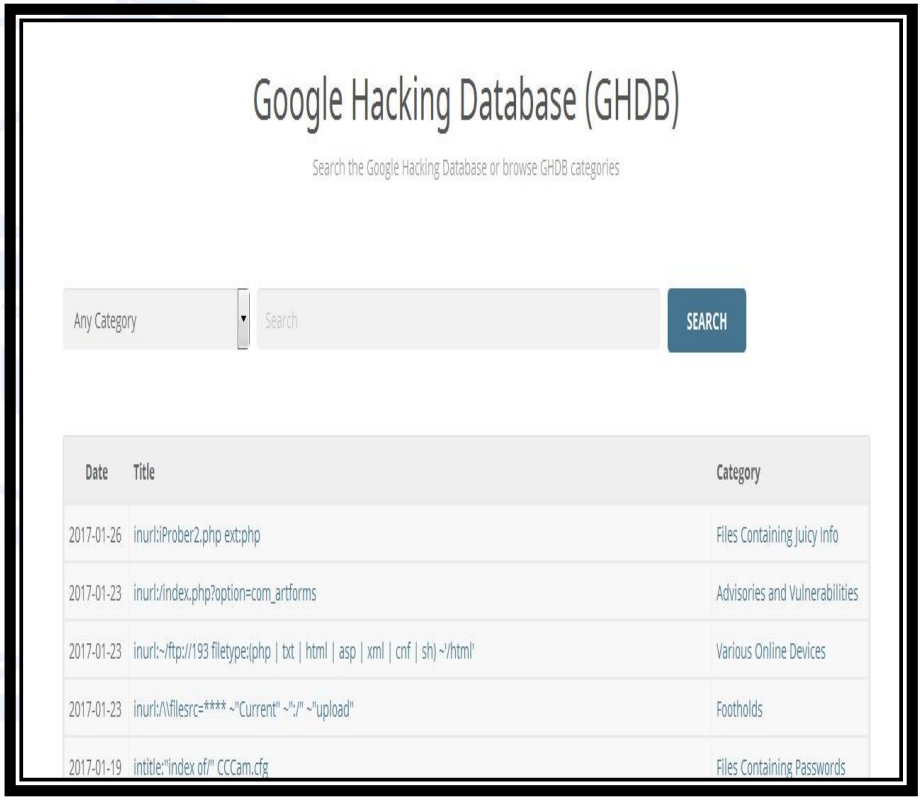
Converged Industrial Network



Systems Are Easy to Target

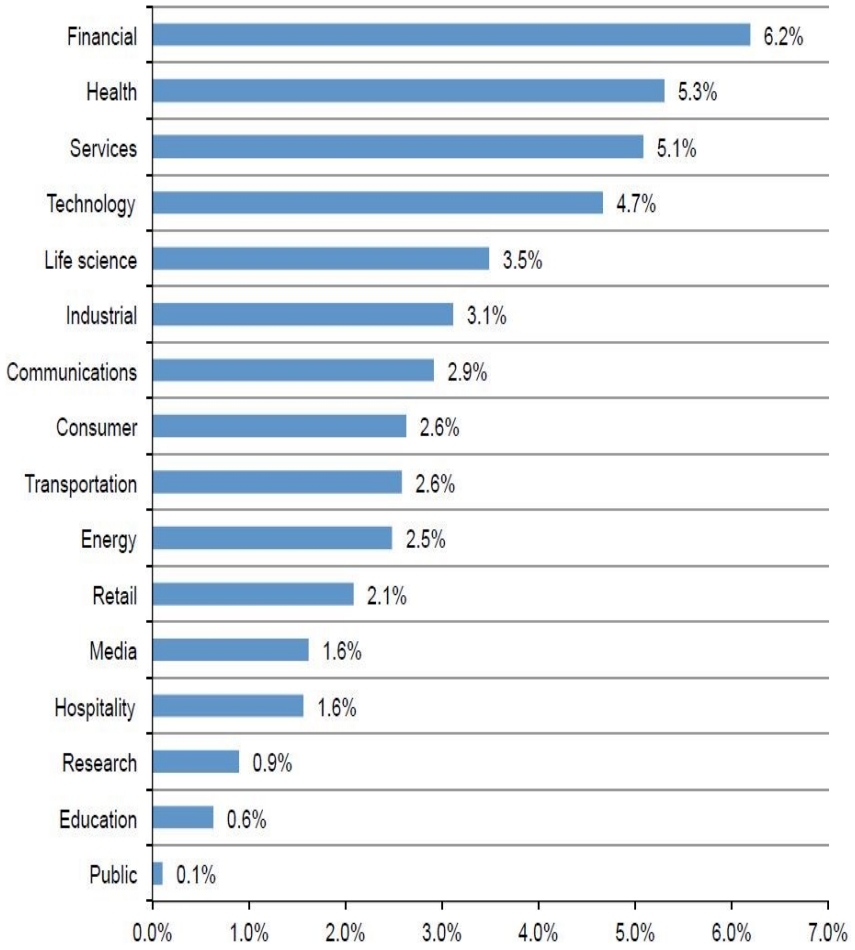
Shodan

Google Dorks



New Industrial Connectivity Brings New Security Risks

- **67 %** off critical infrastructure companies suffered an attack in the last year.
- Many **Security Incident** across all countries
- **Varied motivations**: spying, theft, disruption of operation



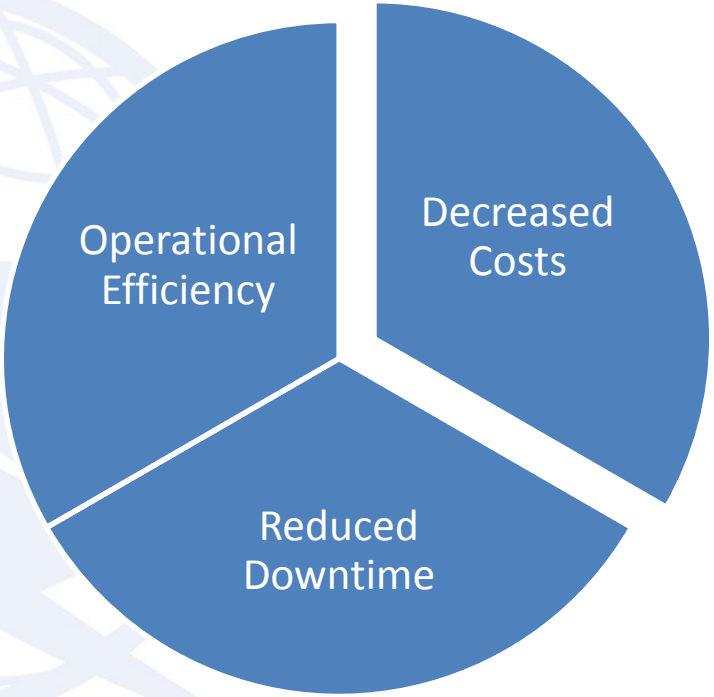
Impact can Be Catastrophic

And they keep coming:

Stuxnet/duqu/flame, watering hole attacks and energetic bears ---!!!!

Ending on a Positive Note

Why this move to connecting devices and IT resources?



…. With this comes
Security Responsibility

Steps To Securing Critical Infrastructure

- **Senior management has to be on board**
  - ✓ Management is in the dark usually and IT can basically do whatever they want
    - Understand Operations
    - Understand Ecosystem
  - ✓ They need to make have objective resources are available
  - ✓ They need to make sure that people are working together
  - ✓ They have to make this a priority

- **To know what you have install**
  - ✓ you can't secure what you have, unless you know what you have
  - ✓ Interview the stakeholders
  - ✓ Collect data

Steps To Securing Critical Infrastructure

- ## Risk Assessment
  - ✓ **Leverage third-party assessments**
    - **Design reviews**
    - **Device security**
  - ✓ **Fix issues early**
    - **Improve product security**
    - **Reduce public breaches and recalls**
    - **Save money time and headaches**

- ## Proper Policy & Procedure
  - ✓ **Build security into the process**
  - ✓ **Train people on what to do … understanding why the policy is their they need to have this understanding when it come to security**

Thank you