Cyber Insider Threat

WINS / FANR workshop
Abu Dhabi, UAE
16 – 18 December 2018

A.B. Keizer
Security Manager
URENCO Nederland B.V.

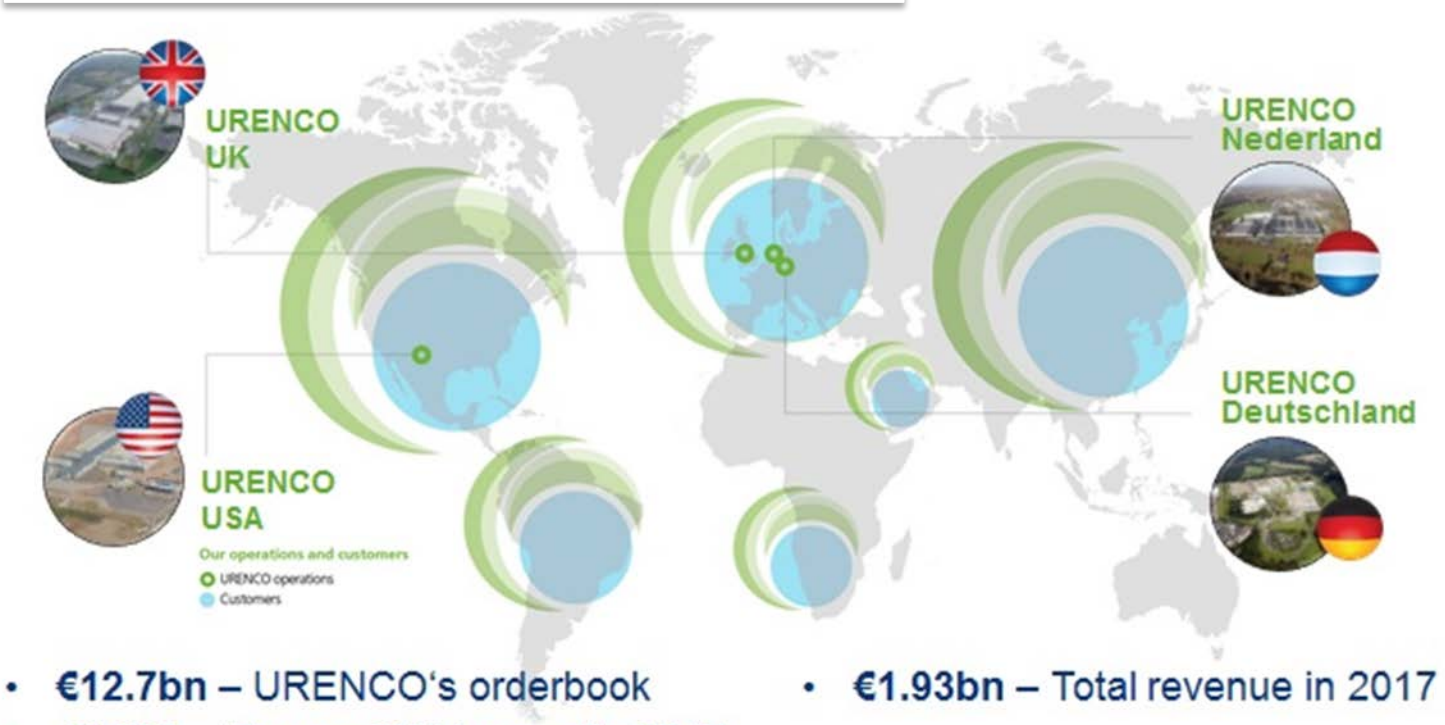
Content

Content

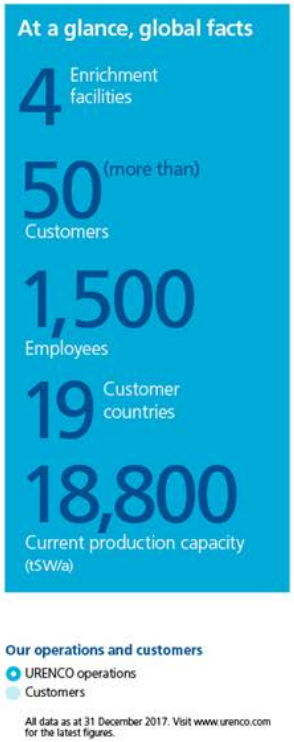
1. URENCO at a glance
2. Regulations and risk management
3. Cyber risk is complex
4. Insiders and insiders
5. Countermeasures
6. Some further advice
7. Challenges

1. URENCO at a glance

URENCO GROUP



- **€12.7bn** – URENCO's orderbook
- **18,800** – Tonnes SWU capacity 2017
- **€1.93bn** – Total revenue in 2017



2. Regulations & risk mgt.

- Nuclear regulations in the Netherlands include a.o.
  - Physical DBT
  - Cyber DBT
  - Both have active and passive insiders as threat actors

- Company risk management
  - Several tools with different abstraction level
  - All include the insider as threat actor
  - (cyber) security risk management follows were possible the general company process

3. Cyber risk is complex

- Data connections
- SAAS & Cloud
- COTS IT Equipment
- OT development
- OT/PP maintenance engineers

This is More than your own staff / more than your own site

4.1 Insiders and insiders

- How many people work at your facility?
- How many others enter your facility?
- Are they all equal in threat?

➔ Map out your users on insider characteristics

	USER GROUP 1	USER GROUP N	ADMIN GROUP 1	ADMIN GROUP N
ACCESS				
KNOWLEDGE				
AUTHORITY				

➔ Apply graded approach in measures

4.2 Insiders and insiders

The intentional insider

- Change settings / data
- Install malware
- Install illegal access
- Remove data

The unwitting insider

- Mobile phones
- USB sticks
- Home work
- Phishing emails

5.1 Countermeasures

Against insiders in your organisation

Against insiders at suppliers / contractors

General countermeasures

5.2 Countermeasures

General countermeasures

- Security screening
  - Governmental security vetting
  - Pre-employment screening
  - In-employment screening / behavioral observation
- Basic cyber hygiene
  - Access rights and privileges
  - Updating and patching
  - Monitoring
- Basic security awareness
  - Security awareness training
  - Recognition of a credible threat
  - Obligation / willingness to report deviations

5.3 Countermeasures

General countermeasures, continued

- Basic monitoring
  - Perception of likelihood of being caught
  - Blocking of unwanted actions
  - Detection of deviations
- Basic tests
  - Phishing email tests
  - Vulnerability scans
  - Penetration testing
- Basic IT architecture / management
  - Apply segmentation, firewalling
  - Invest in tools & manpower for log analysis, SIEM
  - Central and protected back-up storage

5.4 Countermeasures

General countermeasures, continued

- Collaboration with HR
  - Employees with work / home related problems
  - Organizational changes, downsizing, demotion
  - Agree exit process depending on the risk of the person / job title
- Miscellaneous
  - Ensure knowledge is not held by a single person
  - Use DLP technology
  - Ensure life cycle management for your systems

5.5 Countermeasures

Measures against “internal” insider

- Good implementation of need-to-know & need-to-be
- Separation of duties; f.i. between “parametrization” and “authorization”
- Monitor and show you use it (call people to “help”)
- Invest in employee satisfaction
- Attention for management style
- Accessible security department; be on the shop floor
- An open eye….. (insiders are not insiders from one day to the other)
- “Under duress” indication system for limited number of key personnel

5.6 Countermeasures

Measures against the “external” insider

- Require in the contract security measures at the 3rd party
- Include key 3rd party staff in your own security awareness campaigns
- Periodic visits to contractor offices to inspect and explain
- Limit the use of suppliers laptops etc.
- Strict process of software tests and acceptance
- Strict escorting for suppliers / contractors

6. Some further advice

Some further advice

- Pursue a multi-disciplinary approach (SEC, HR, Operations, Maintenance, etc)
- Invest in employee satisfaction
- Ensure good management style
- Facilitate reporting of deviations (culture & system)
- Consider behavioral observation
- Consider predictive profiling
- Be aware of the traditional traits, like very high loyalty, little to no time off for vacation etc.
- Consider psychological testing for risk prone behavior
- Consider alcohol & drugs testing
- Consider NMAC in your approach

7. Challenges

Challenges

- Recognition of the risk (at general management)
- Balance between innovation and risk
- Security awareness, especially with suppliers / contractors
- Loyalty, especially of suppliers / contractors
- The amount of logging information
- Big brother is watching you emotion
- Reorganization, down-scaling periods
- Organize not only the defense, but also the recovery
- And your “first responders” and CMT for such cases

Thank you for your attention

Questions, remarks, suggestions?