

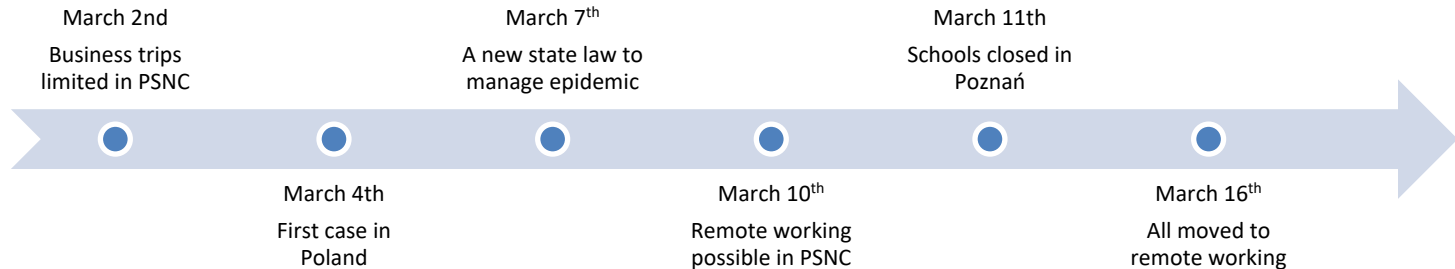


## Continued NOC operations in the face of a pandemic

Szymon Trocha

Poznań Supercomputing and Networking Center  
SIG-NOC11, March 25th, 2020

## General timeline and company responses



- Only single key person from each team physically present in the premises
- All non-outage related trips postponed
- NOC specific
  - NOC is somehow separated by itself
    - 2 separate NOCs
      - 1+2 persons on duty
      - Separated by locations and services
  - But BMS and remote-hands require us to keep NOC staff

## Personnel safety first

- Placed hand sanitizers in NOC rooms
- Placed disinfectant in NOC rooms for equipment cleaning
- Increased the frequency and range (desks, door handles) of cleaning operations
- Provided protective gloves
- Changed colocation visit procedures to limit the in-building walks
  - Provide additional guidelines to customers and urge to postpone unnecessary maintenance
- Used thermal cameras where possible (still in testing)
- **Maintain communication to NOC staff**



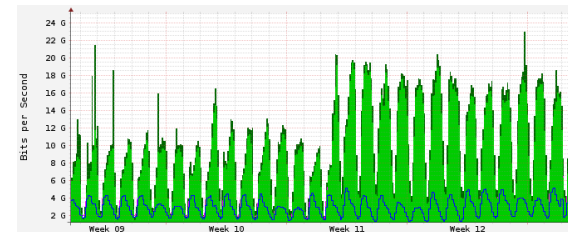


## Challenges

- NOCs need to maintain physical presence
- NOC staff are not dedicated engineers
  - Cannot work remotely
- Contingency planning anticipates replacement rules for missing shifts
  - Achieved via NOC personnel replacement
  - Exceptions covered by members of Network Management Team and Services Team
    - Still physically present in PSNC premises
  - But not full NOC closure
- Can't do remote
  - BMS
  - Fire detection and distinguishing system
  - Manual interventions e.g. wrt power outages

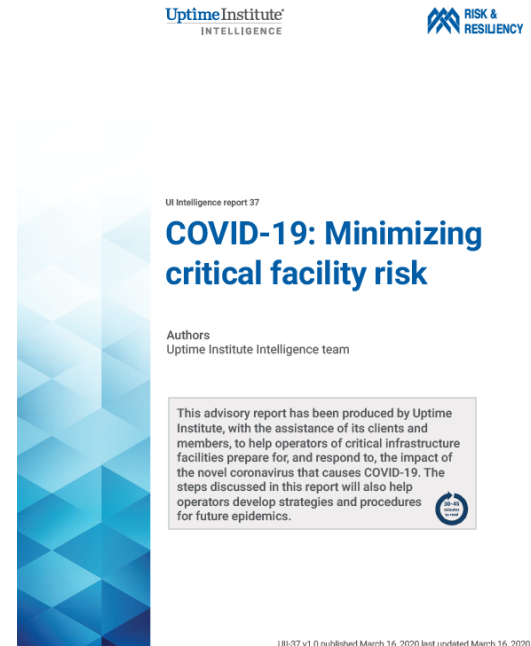
## Contingency planning

- Reviewed Business Continuity Plans
  - Some already ready for ISO-27000
  - Reviewed risk assessment
  - Immediate UPS and generator tests (some failed ☹ )
  - Reviewed plans for switching off services in case of longer power outages
    - Keep key infrastructure running as long as possible
- Intensified network and services monitoring
  - Network impact is not that significant
  - Increased demand for services (VC)
  - Need to observe the government rules that apply for network operator
  - Watch for possible DoS attacks for key services



## Additional materials

- By Uptime Institute
  - COVID-19: Minimize Critical Facility Risk On-Demand Webinar  
<http://go.the451group.com/yGODYJmg0o0eYYA0jS00010>
  - COVID-19: Minimizing Critical Facility Risk Report  
<http://go.the451group.com/gC0Yjge0J10GY0oD000UOm>







# Poznań Supercomputing and Networking Center

affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences,

ul. Jana Pawła II 10, 61-139 Poznań, POLAND,

Office: phone center: (+48 61) 858-20-01, fax: (+48 61) 850-25-01,

e-mail: [office@man.poznan.pl](mailto:office@man.poznan.pl), <http://www.psnc.pl>