Communicating across borders in times of crisis

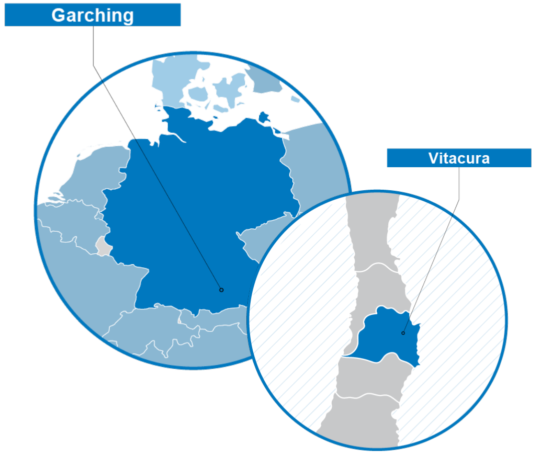
Lessons learnt from a cyber incident at ESO

Anna-Lynn Wegener

Head of Communications, ESO

What is ESO?

- An **intergovernmental organisation** with 16 European Member States
- We **design, build and operate telescopes** in the Chilean Atacama desert and **promote international collaboration** in astronomy.



Data Classification: ESO external

How it all began…

Data Classification: ESO external

Here is what had happened…

- ESO was informed by intelligence services that they had information suggesting that ESO’s network had been successfully compromised

- No information if the intruders were still in the ESO’s IT infrastructure or had successfully stolen data

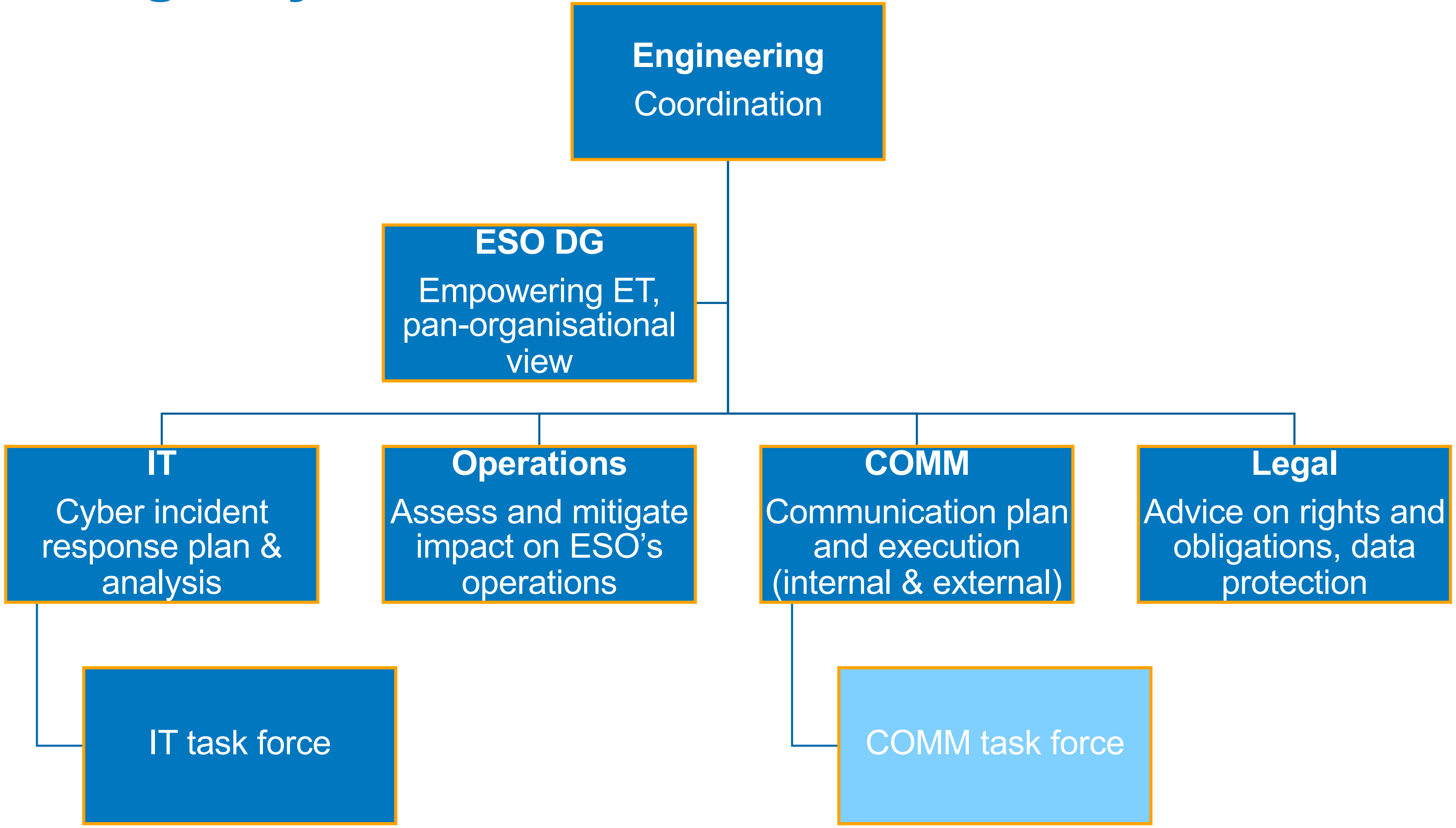
- Reason to believe that the intruders were most probably after insights into projects, technologies and operations (rather than a ransomware attack or personal data theft)

Incident response

- Emergency Team to develop and execute an incident response plan (guided by cyber security consultants).
- The requirements on the plan were:
  - Do the utmost to prevent the hackers from knowing that they have been discovered to avoid any damage, data theft or encryption as part of their exit strategy
  - Minimize the impact on ESO's business and operation

Data Classification: ESO external

The Emergency Team



Engineering

Coordination

ESO DG

Empowering ET, pan-organisational view

IT

Cyber incident response plan & analysis

Operations

Assess and mitigate impact on ESO's operations

COMM

Communication plan and execution (internal & external)

Legal

Advice on rights and obligations, data protection

IT task force

COMM task force

Data Classification: ESO external

Working together in the Emergency Team

- **Communication protocol** :
  - In person, via Teams calls (not Teams messages), phone calls and private email addresses.
  - No use of collaborative documents saved on shared drives. Local storage of documents.
  - No communication beyond the ET and IT task force!!!

What worked:	To avoid:
Daily ET meetings for updates & exchange	Bilateral communication leads to disconnected parallel action & knowledge and mental overload.
Clear roles & letting experts do their jobs …	… much negotiation between different perspectives, cultures and needs.
Small Emergency Team helped with keeping confidentiality …	… but not with mental overload, bringing in required knowledge and sharing tasks.

Incident response plan

- Intense preparation: controlled incident response with a lead time of ca. 10 days.
- Controlled disconnection of ESO’s network from the internet for an organisation-wide systems upgrade, analysis and necessary troubleshooting.
- Estimated downtime: 2pm Friday 17 May to 8am Tuesday 21 May (Pentecost weekend)
- It was unclear how long this might take and what we would find.

Data Classification: ESO external

What does an internet shutdown mean for ESO?

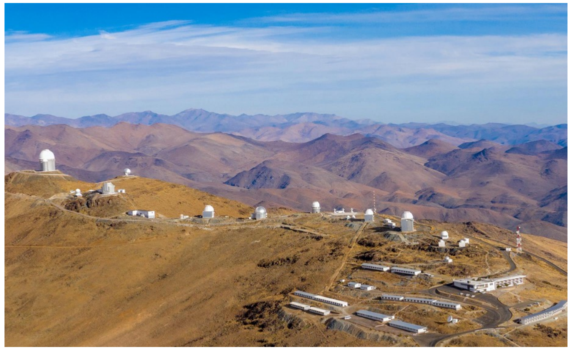
ESO Headquarters in Garching, Germany

ESO's science, administration and technology centre

ESO Supernova Visitor Centre & Planetarium (operating on weekends)

ESO Offices in Santiago, Chile

ESO's hub for science and technology in Chile



3 ESO observatory sites in the Chilean Atacama desert

>150 people operating on 24/7 shifts. Very isolated, limited mobile network. Satellite phones & radio.

Thanks to local networks: most work happened as normal.

Data Classification: ESO external

What does an internet shutdown at ESO mean for the outside world?

- ESO's websites and all related services for **astronomers** unavailable:

> 'Due to an important system upgrade, ESO's communication systems are currently unavailable. This includes WIFI connection, ESO websites and email communication with people outside the ESO network. We apologise for the inconvenience and are working hard to be back online as quickly as possible.'

- **Public visitors**: ESO Supernova Visitor Centre and at observatories.
- **Visiting astronomers** and **operators of hosted telescopes** at observatory sites cut off.
- … many more, not all predictable!

Data Classification: ESO external

The internal communication challenge

- Many activities affected: staff needed information to inform external stakeholders to mitigate impact.
- Staff could not be informed before the shutdown to contain risk of setting off the intruders.
- With digital comms channels down, no way to inform staff at all locations after 2pm on Friday.

- **Contemplated solutions**:
  - 5 simultaneous local all-hands meeting at Friday 2pm? But what about people working remotely?
  - Messages to cell phones or personal email addresses? But no central register.
  - Letters to staff home addresses sent 2-3 days prior to shutdown? But fast-changing situation, limited reliability and many people are not at home.

- **Final solution and game changer**: IT found a possibility to keep MS Teams connection selectively open to allow internal communication across sites during shutdown.

Internal communication log on 17 May

Time	Action
20.00 CET, 16 May	DG sends cryptic email invite to all staff for urgent all-hands meeting.
	[speculations through the roof, but no major leak]
13.45 CET, 17 May	Internet shutdown
14.00 CET	• All-hands assemblies at all sites, streamed from HQ via MS Teams • Inform staff about the situation, staff's role in the upgrade of their machines etc. • Discuss implications for staff, addressing worries, communication protocols, building understanding and trust!
14.45 – 15.45 CET	60 minutes Q&A with staff
	[the longest and most heart-felt applause for ESO IT]
16.00	Summary message through 'All ESO Team' on MS Teams.

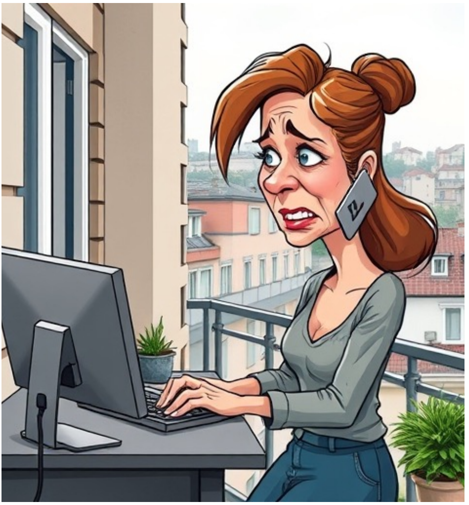
A looooong weekend

ESO IT

Most ESO staff

At the observatories

ESO Communications

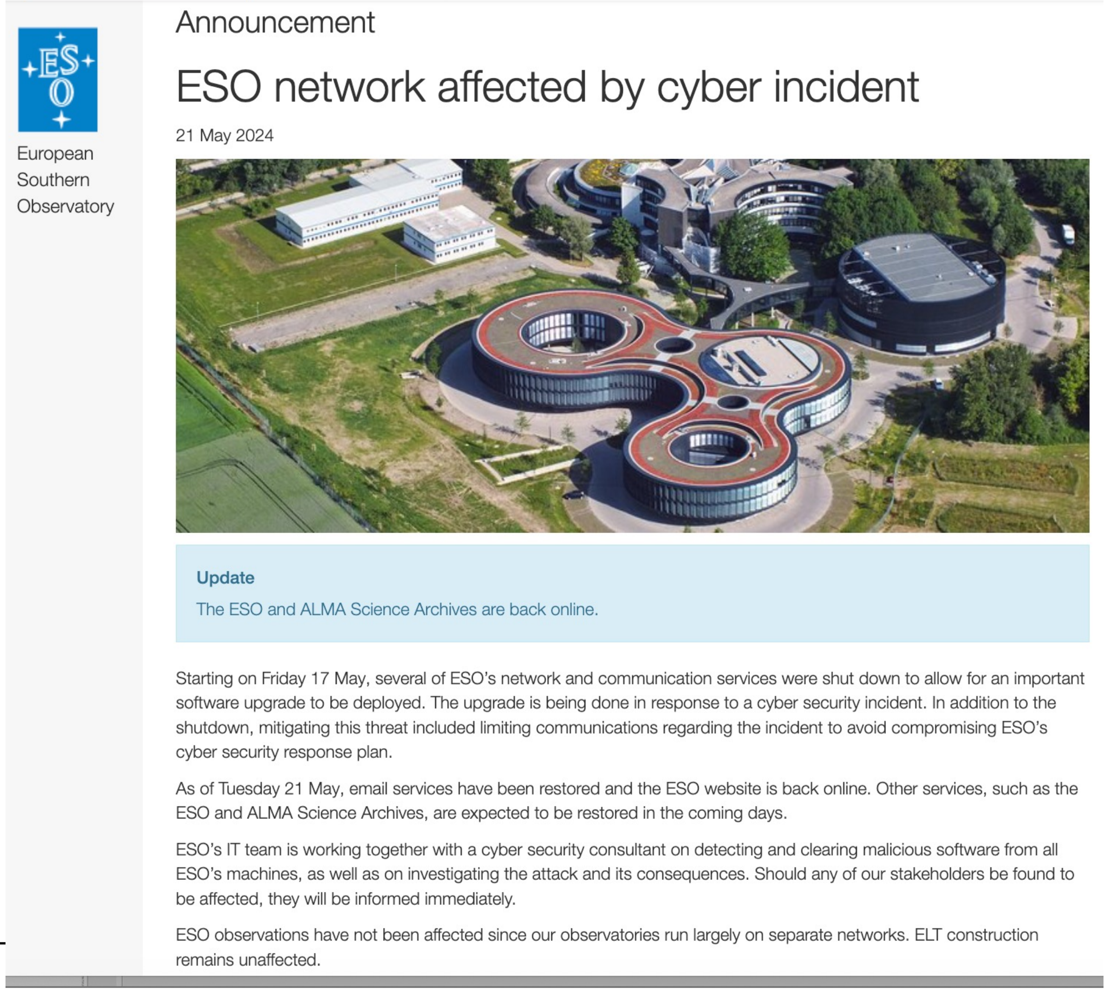


The rest of the world…

Data Classification: ESO external

Internet back: Tuesday afternoon

- Inform staff about services running and the results of the analysis
- Public announcement about the incident and ESO's response
- No major inquiries by the media, some by users/community
- Expressions of curiosity, solidarity and understanding on social media
- Targeted communication with impacted stakeholders



European Southern Observatory

Announcement

ESO network affected by cyber incident

21 May 2024

Update

The ESO and ALMA Science Archives are back online.

Starting on Friday 17 May, several of ESO's network and communication services were shut down to allow for an important software upgrade to be deployed. The upgrade is being done in response to a cyber security incident. In addition to the shutdown, mitigating this threat included limiting communications regarding the incident to avoid compromising ESO's cyber security response plan.

As of Tuesday 21 May, email services have been restored and the ESO website is back online. Other services, such as the ESO and ALMA Science Archives, are expected to be restored in the coming days.

ESO's IT team is working together with a cyber security consultant on detecting and clearing malicious software from all ESO's machines, as well as on investigating the attack and its consequences. Should any of our stakeholders be found to be affected, they will be informed immediately.

ESO observations have not been affected since our observatories run largely on separate networks. ELT construction remains unaffected.

Data Classification: ESO external

Lessons learnt I

- Plans and preparation are great…
  - Existing crisis management structures, processes and tools (ET, clear roles, approvals, comms channels), an inventory of affected operations and expected impacts.
  - Existing cyber security strategy and consultancy contract.
- … but flexibility is required!
  - Cases are different and the devil is in the details.
  - Fast-changing situation.
  - Established channels and team processes might not work.
- It’s going to be messy and stressful, deal with it!

Lessons learnt II

- Relationships are key!
  - Build them in good times, so you can rely on them in tough times!
  - When in crisis, be kind and trust your colleagues! Control does not scale well under stress.
- Person-to-person comms is the basis for everything and it is very effective.
  - Staff need enough info to inform stakeholders.
- Balance confidentiality and transparency carefully
  - Diverse expertise, skills and brains vs needs for confidentiality and efficiency.
  - Unnecessary alarm vs understanding and support.
- People pull together in times of crisis!
  - Lots of engagement, support and appreciation.

Thank you!

Anna-Lynn Wegener
Head of Communications, ESO
awegener@eso.org

@ESOAstronomy

@esoastronomy

@ESO

european-southern-observatory

@ESOobservatory

The week after: Internal communication

- Tuesday 21 May: Email update on analysis and troubleshooting over the weekend.
  - No internet connection yet. Gradual reconnection of the systems and restoration of tools.
  - Work continued (on- and off-site) within the restrictions of limited connection.

- Daily email updates to staff announcing systems being reconnected and results of analysis.

- 7 June: incident wrap-up in all-hands meeting.
  - Analysis results and impact on ESO and stakeholders.
  - Future mitigation and preparedness plans.
  - More Q&A and thank you’s to staff.

Data Classification: ESO external

The ‘right’ level of transparency?

- Legal constraints and risk to expose critical technical information.
- Informing vs alarming stakeholders while analysis was ongoing and there were no answers yet.
- ET members comfortable with different levels of transparency.
    - Internally: maximal possible transparency to enable staff to work, inform contacts and to have understanding and buy-in.
    - Externally: minimal holding statement while analysis was going on, the impact on stakeholders was estimated, targeted direct communication with stakeholders.
- Risk of dichotomy: information leak and reputational damage!
- Mitigation: close monitoring, scenario planning and detailed Q&As.