CRAIG MORRIS

APPLYING LESSONS LEARNED FROM CYBERSECURITY INCIDENTS IN OIL AND GAS TO OTHER CRITICAL INFRASTRUCTURES

AISA

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

CHANGE THE RULES
UP THE GAME
AUSTRALIAN CYBER CONFERENCE 2019

AISA AWARDS

AISA 20 YEARS

DISCLAIMER

- My personal experiences - Stories from the trenches
- No technical details
- Lessons learned to help asset owners prepare for similar incidents

"Those who do not remember the past are doomed to repeat it."

– George Santayana

***Doha, Qatar – 30 August 2012**: RasGas Company Limited (RasGas) confirms the company's office computer systems were affected by an unknown virus on Monday 27th August 2012. Key impact remains in the administrative IT System; Operational Systems on site and offshore are secure. The production and supply of Liquified Natural gas (LNG), pipeline gas and associated products is uninterrupted.*

A specialist RasGas IT team, in collaboration with technical experts, is working to resolve the issue as soon as possible.

Gulf Times

Houston, we have a problem

- Test, update BCP and IR plans regularly
- Store & maintain plans, docs, images securely
- Understand your infrastructure

- Identify “Crown Jewels”
- Update and test DRP plans based on “Crown Jewels”
- Review storage, recovery capabilities
- Audits and Single file recovery **!=** Testing

Show me the money!

- Establish support contracts for critical suppliers & systems
- Review / renegotiate as needed
- No free stuff !

- Analogue is still needed. Whiteboards, Fax etc
- Manual processes – exist, tested and approved?
- Backup internet connectivity

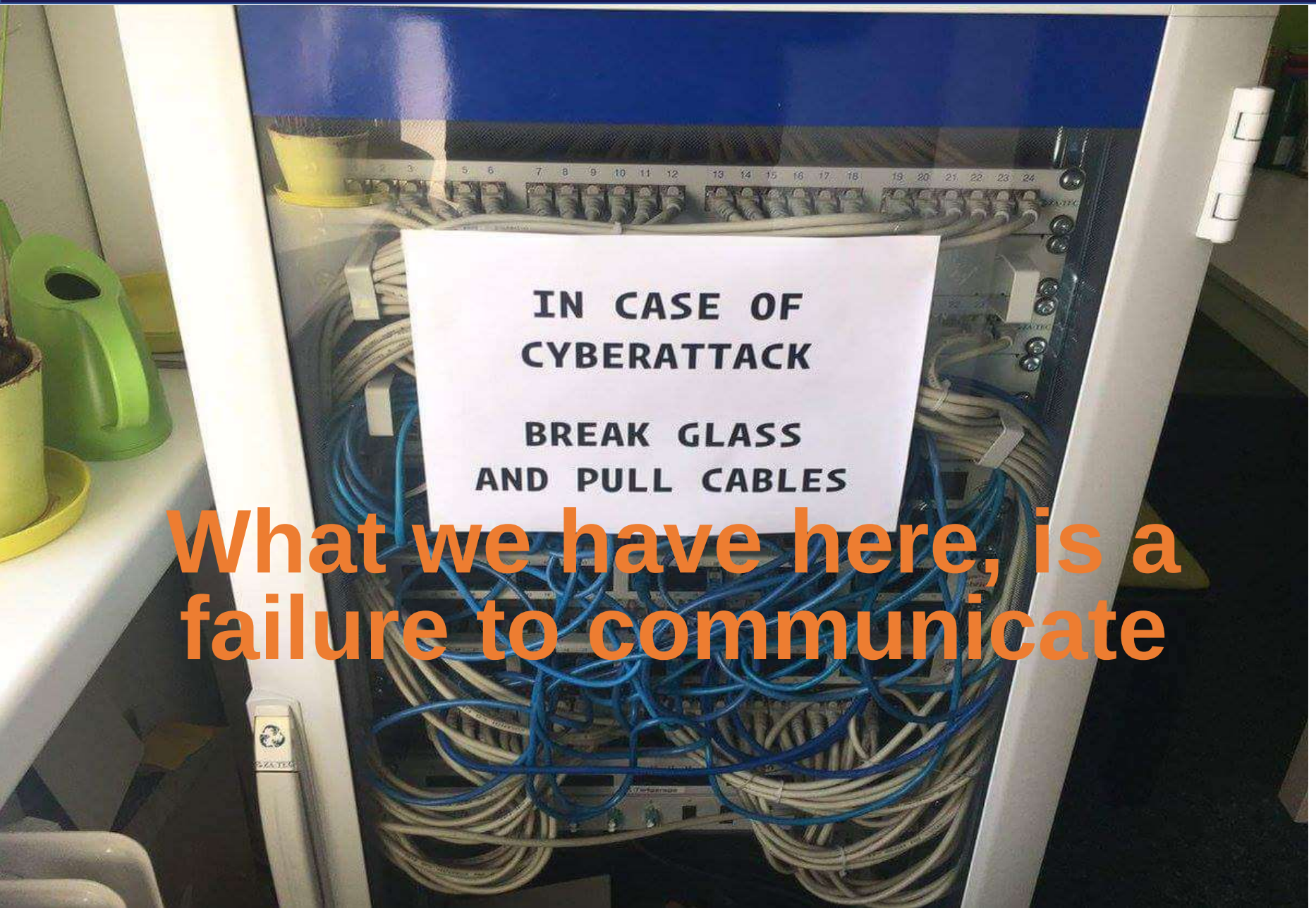
Who are you gonna call?

- Manage via Emergency Management Team (with PR & Legal)
- Open, transparent, reassuring
- Don’t let IT handle communications – ever ☺.

CIRT Leader – Protect the team

Food, transport, accommodation

Rosters, rotations, rest



What we have here, is a failure to communicate

- Understand network paths and dependencies
- Robust O.O.B communications
- User communication methods

- Don’t ignore Change Management
- Change Management ‘Lite’ – risks, details, authorisation
- Update processes, builds with changes

Putting the band back together

- Continue to train and rehearse, realistic scenarios
- Update plans when business objectives change
- Ensure equipment etc available and functioning

Prior Planning Prevents Poor Performance

- Identify and protect "Crown Jewels"
  - Identify and assess critical processes and systems
- Automate response and recovery processes & capabilities
  - Automation and Immutability for infrastructure, backups
- Continuously update and test plans (DRP, IR, BCP)
  - Exercise regularly with realistic scenarios and independent review
- Analog capability, manual processes
  - Identify requirements, identify and verify manual capability
- Look after your team
  - Training, protect them, feed them occasionally

Questions?

https://www.linkedin.com/in/camorrisaus/

Actions

Next Week

- Review and update your existing IR and DRP plans esp. contacts
- Create/Update secure offline copies of plans, tools, images
- Schedule and run a response exercise (IT and Business) – TTx

Next 3 Months

- Identify Crown Jewels
- Verify vendor support arrangements
- Review and update your BCP and associated plans (and capabilities)

Thank You