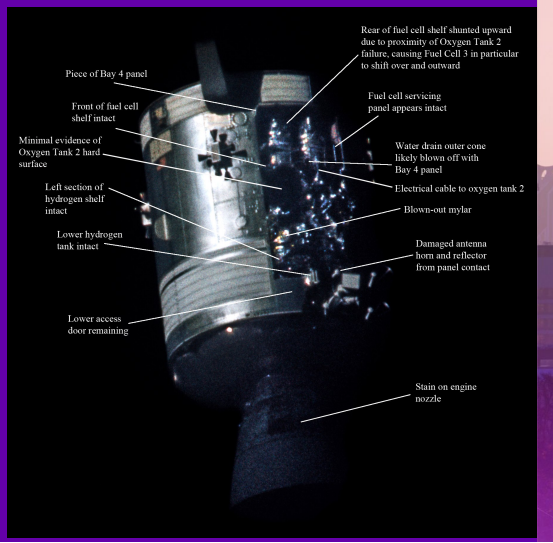
Failure is not an option- Houston

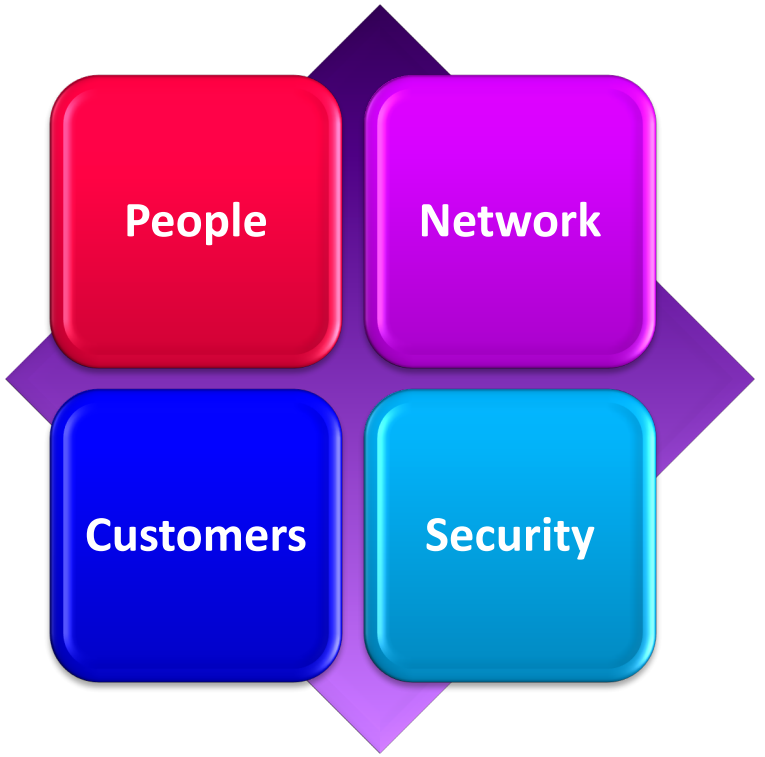
Neil J. McRae – BT

Virtual UKNOF

11th May 2020



Agenda



Houston – the project name to call when disaster strikes

“I believe this will be our finest hour”

Gene Kranz, Flight Director Apollo XIII

People

Non Operational

Closed Our Shops – 1.5K retail staff issued with laptops to support call centres.

Closed Offices

Global Impact (India, other countries)

70K Teams users

80K Unique VPN users

Paying all staff irrespective of situation

Huge effort on mental wellbeing.

562% increase using video in conferences.

Operational Sites

Operation Centres

NOC migrated to home working second week of lockdown

Shifts adjusted to help with nightshift etc

Call Centres – Social Distancing, Free meals
Majority migrated to work from home – some hard to do- 8000 agents moved to WFH.

Global Centers – also working from home

Field

Category 0
Service Impacting

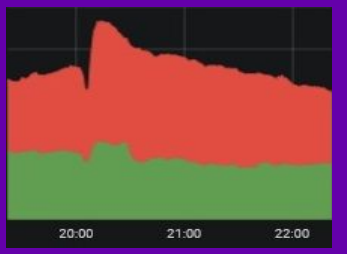
Category 1
High Priority

Category 2
Priority

Category 3
Complete If Possible

Category 4
Suspended

Network - Covid-19 Traffic Update – Start



26/03 8pm NHS – Clap for our carers
Short drop in traffic

23/03 8pm Prime Minister's TV address

17.5Tb: highest ever peak achieved on the BT network.
Maximum capacity of the network is higher still, and we have plenty of additional headroom.

I couldn’t think of a polite slide title- Covidiots?

Engineers across industry physically and verbally abused

Infrastructure set on fire

Utter madness and totally unacceptable.

Customers

40K VPN platform for Lloyds Bank

40K VPN seats in Spain

Over 500,000 VPN seats provided

150M minutes per day increase on IPX

Cloud Contact Centre Platform traffic doubled.

All nightingale hospitals connected with BT Fibre

Coverage enhanced for 4 Nightingale Hospitals

Mobile Coverage for 16 field hospital enhanced.

BT Conferencing traffic doubled

Partnership with ITV on learning.

Security - Vishing

Top 5 Covid 19 vishing scams

1. **Fake test kits scam** – someone may call claiming to offer free Coronavirus testing kits and will ask you for your personal information and health insurance details. A common version of this scam targets diabetic individuals that are higher risk, where a scam caller will offer both a free Coronavirus test kit and a free diabetic monitor.

2. **Insurance scam** – scam-callers posing as employees from the Government Insurance will ask you for sensitive information, such as your social security number and bank account information, over the phone as a precondition to receive government money. Remember the government would never make unsolicited phone calls asking for personal information and money, and especially would not put pressure on you or threaten you.

3. **Charity scam** – you may get a call from someone claiming to be from a charitable organisation which is collecting donations for individuals, groups or areas affected by Coronavirus. The caller will ask you to send cash donations in the mail, by wire transfer or by gift card.

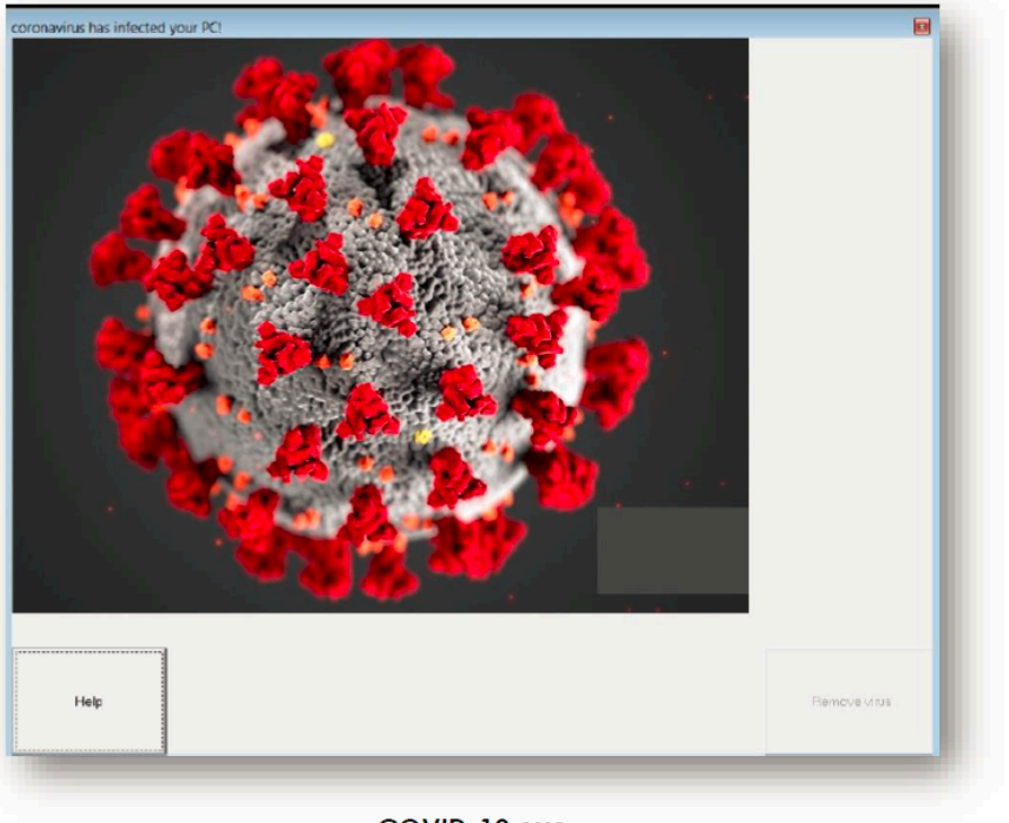
4. **Healthcare provider scam** – scam-callers pretending to work for a healthcare provider will tell you that a relative or friend has been treated for Coronavirus, and then demand immediate payment for treatment before threatening legal action if you don't pay. Healthcare providers would not contact you this way.

5. **Student loan scams** – you receive a call to tell you that new measures due to the Coronavirus outbreak will have an effect on your student loan, and that you need to ring a different phone number to find out how the new measures will impact your future payment obligations. If you ring this number, a scammer may ask you for personal information like your social security number and credit card details.

Malware

39 different Malware families are being used by threat actors leveraging Covid-19 phishing attacks.

- **Hancitor –** A downloader which has tried to penetrate the BT estate in a malspam campaign (see Phishing slide). Hanicitor has been known to be an entry point for Gozi, Ursnif and Pony.
- **"Coronavirus" –** Replaces the 'master boot record' of a computer so that it prevents the operating system from starting and displays a ransom note or other message instead. Being distributed as the COVID-19.exe file.
- **Revil (Sodinokibi) -** Ransomware exploiting unpatched Pulse Secure VPNs targeting managed service providers. Used in recent attacks against healthcare and medical research firms.
- **Emotet –** Efficient downloader, C2 difficult to detect, utilised by multiple threat actors. Now using a Corona themed template.
- **LokiBot-** Information gathering tool. Collects Passwords, Crypto wallets, screenshots, keystrokes and cookies.
- **Trickbot-** A Trojan-like spyware program that has been used primarily to target banking sites. Heavily used in Italy. Using a WHO lure.
- **AZOrult –** Trojan used to steal info, sold on forums for $100. Used in a fake map that claims to track the pandemic.
- **SpyNote RAT –** Remote access trojan for Android devices.



COVID-19.exe