# Cyber resilient operations in healthcare: Keeping the clinic running under cyber attack

Juha Eskelin
2019-02-14

Bittium

In the open responses to the Digital Health NHS Cyber Survey, December 2016, one NHS IT director said “it’s just a matter of time before a trust is taken out by a cyber security attack”.

In October 2016 Lincolnshire and Goole NHS Foundation Trust had to declare a critical incident, revert to paper systems and cancel operations for three days after its systems were struck by a CryptoLocker attack.

In May 2017 80 out of 236 hospital trusts across England were affected by the WannaCry ransomware attack.

Digital Health NHS Cyber Security Survey Report, 2016

https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Bittium

# Critical infrastructure security and resilience

The ability to *prepare* for and *adapt* to changing conditions and *withstand* and *recover* rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents

Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, February 2013
https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf

Bittium

# NIST Cyber resiliency techniques

- Adaptive response
- Analytic monitoring
- Coordinated protection
- Deception
- Diversity
- Dynamic positioning
- Dynamic representation
- Non-persistence
- Privilege restriction
- Realignment
- Redundancy
- Segmentation
- Substantiated integrity
- Unpredictability




https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

# Case: Cyber resilience under WannaCry

# Case: Cyber resilience under WannaCry

- Cancer hospital had a resilience plan in place
- NHS shutdown caused by WannaCry did not impact cancer clinic operations
- Multiple measures had been taken to prepare for disruptions, to withstand the attack and to adapt to changing conditions

# Case: Cyber resilience with Bittium SafeMove

- Use of SafeMove Access Control server for limiting access exclusively to NHS services
- Use of cellular modems in laptops/tablets to find alternate connection paths with hospital campus network/Wi-Fi shut down
- Use of SafeMove automated disaster recovery server discovery to access critical services from DR site
- Use of SafeMove Field Office Router to provide secure ad-hoc Wi-Fi access for non-cellular capable devices
- Use SafeMove Analytics to discover suspicious network activity

Bittium

# Case: Cyber resilience with Bittium SafeMove

- Use of SafeMove Access Control server for limiting access exclusively to NHS services
- Use of cellular modems in laptops/tablets to find alternate connection paths with hospital campus network/Wi-Fi shut down
- Use of SafeMove automated disaster recovery server discovery to access critical services from DR site
- Use of SafeMove Field Office Router to provide secure ad-hoc Wi-Fi access for non-cellular capable devices
- Use SafeMove Analytics to discover suspicious network activity

**Privilege restriction**
**Diversity**
**Dynamic positioning**
**Redundancy**
**Analytic monitoring**

# NHS UK WannaCry learnings for resilience

Bittium

# Lessons learned: Resilience

Local organisations' business continuity and disaster recovery plans should include the necessary detail around response to cyber incidents

The business continuity and disaster recovery plans should be regularly tested, reviewed, updated locally

Develop scenarios to ensure to manage a coordinated or multiple attack, for instance, a terrorist bombing attack is combined with a cyber attack.

https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

# Contact us.

www.bittium.com
firstname.lastname@bittium.com