

A serene landscape featuring a calm lake reflecting the sky and surrounding trees. In the foreground, there are reeds and rocks. The sky is a mix of blue and orange, suggesting a sunset or sunrise. The overall mood is peaceful and natural.

# 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.



# 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

# NIST Cyber resiliency techniques

**Adaptive response**

**Diversity**

**Realignment**

**Analytic monitoring**

**Dynamic positioning**

**Redundancy**

**Coordinated protection**

**Dynamic representation**

**Segmentation**

**Deception**

**Non-persistence**

**Substantiated integrity**

**Privilege restriction**

**Unpredictability**



# Case: Cyber resilience under WannaCry

The background of the slide is a dark blue gradient on the left, transitioning into a complex, glowing network of interconnected nodes and lines on the right. The nodes are represented by small dots in various colors (blue, yellow, orange), and the lines are thin, light blue. A bright, multi-colored light flare (blue, yellow, orange) emanates from a central point within the network, creating a sense of energy and connectivity. The overall aesthetic is futuristic and technological, representing a global network or data flow.

**Bittium**



# 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



# 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

The background of the slide is a complex digital network. It features a dark blue and black space filled with numerous small, glowing blue and yellow dots. These dots are interconnected by a web of thin, light blue lines, creating a mesh-like structure. A prominent, bright blue light source is visible in the lower-left quadrant, casting a strong glow and creating a lens flare effect. The overall aesthetic is high-tech and futuristic, suggesting themes of cybersecurity, data networks, and digital 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](http://www.bittium.com)

[firstname.lastname@bittium.com](mailto:firstname.lastname@bittium.com)

# Bittium