When patching gaps became front-line service disruption

National Health Service in England | England | National Health Service | Attack and disruption May 2017 | NAO report October 2017

TRUSTS AFFECTED	CANCELLED APPOINTMENTS	A&E DIVERSIONS	ATTACK WINDOW
At least 80 of 236	**Est. 19,494**	**Five**	**12-19 May 2017**
S01	S01	S01	S01

DOCUMENTED EVENT

The WannaCry ransomware attack affected NHS services in England from 12 to 19 May 2017. The NAO reported that at least 80 of 236 trusts were affected: 34 were infected and locked out of devices, while 46 were not infected but reported disruption. NHS England identified 6,912 cancelled appointments and estimated approximately 19,494 in total. Five accident and emergency departments diverted patients. Most infected NHS devices were unpatched supported Windows 7 systems; unsupported Windows XP devices were a minority of identified issues. [S01]

NFRISK SCENARIO ADAPTATION - NOT AN EXTERNAL FINDING

Critical service providers receive security alerts and patches, but cannot demonstrate implementation across distributed estates, embedded devices and local organisations before a rapidly spreading incident tests the gap.

STRESS-TEST QUESTIONS

01 Can management prove critical patches are implemented, not merely distributed?

02 Which essential services depend on unpatchable or embedded devices?

03 Can the organisation coordinate safely when email and core systems are unavailable?

04 Who verifies that cyber alerts produce implemented remediation across every accountable organisation?

CONNECTED RISK

Operational Resilience & Delivery Risk (primary)
Data & Control Integrity (contributing)
Technology & Cyber Risk (contributing)

FRAMEWORK RELEVANCE

NIST Cybersecurity Framework lens: Protect & Recover
NFRisk maps patch assurance, dependency visibility and coordinated recovery to the NIST Protect and Recover functions. This is a retrospective analytical mapping, not an NAO classification. [S03]

NFRISK PRACTITIONER INTERPRETATION

Cyber resilience is an evidence problem as well as a technology problem. Boards need verified patch status, exception ownership, dependency visibility, workable isolation and tested service-continuity communications.

PRIMARY-SOURCE REGISTER

S01 UK National Audit Office (2017)
Investigation: WannaCry cyber attack and the NHS
S03 COSO / Basel Committee / NIST (2017)
Authoritative risk-management framework referenced in the...

EVIDENCE BOUNDARY Official findings are separated from the institutional scenario, framework interpretation and NFRisk practitioner view.