The WannaCry Attack: An Evaluation of Centrally Mandated Information Governance for the English NHS and Local Government

Tony Leary

Technical Report

RHUL–ISG–2020–5

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

In May 2017, a strain of ransomware called 'WannaCry' infected 32 National Health Service (NHS) trusts in England. It was able to self-replicate and spread via data networks, including the NHS national data network (N3). The NHS's report on the incident noted that all English local authorities (LAs) reported being unaffected, despite also being connected to N3. Neither the NHS report nor the subsequent UK Parliament report sought to explain why LAs avoided infection. This project aims to answer that question by evaluating the relative strengths and weaknesses of the centralised security governance systems in place for NHS trusts and local government organisations, both before and after the WannaCry attack. Publicly available data on historical security breaches for NHS trusts and LAs are also analysed for patterns of security control failure that may indicate NHS trusts were at a higher risk of infection. The application of a standard information security control set, ISO/IEC 27002:2013, enabled the different information governance systems and security breach reporting data to be more easily compared.

The results indicated that the NHS's centralised governance in place at the time of the WannaCry attack was weaker than the equivalent governance applying to local authorities. The changes in NHS governance since the WannaCry attack address these weaknesses, while implicitly confirming their existence. The security breach data revealed no significant variation in the root cause control failures for either the NHS or LAs; however, the variation in data focus and quality limits this project's confidence in stating this authoritatively. It is recommended that the UK government standardise its security breach reporting to ensure that root cause data is consistently recorded, allowing standard security controls definitions, such as ISO/IEC 27002:2013 Annex A to be more easily applied to breach data. A standard data set could highlight areas of strength, or weakness, in information governance across government; guidance can then adapt accordingly.