

James Kinross
Senior Lecturer
Department of Surgery & Cancer
Imperial College London
10th Floor, QEQM Building
St Mary's Hospital
London
W2 1NY

j.kinross@imperial.ac.uk

British Medical Journal

30th May 2017

Dear Editor,

Many thanks for considering the publication of this article in the BMJ. We would like to thank the peer reviewers for their comments. As discussed with the Editors we have updated the paper in light of the recent WannaCry attack, and also aimed to focus it more specifically on practical steps and solutions to the threats and risks described. We have also edited in light of our recent invited BMJ Editorial to ensure the same messages are not merely repeated. We hope a combination of the updated text and figures now provides a clear overview of this important subject area, and highlights some key threats and solutions.

We have further updated the paper to reflect the comments from the reviewers, and have addressed their specific comments as outlined below.

If there is anything else further that you would like to discuss or clarify, or if it requires further revision please do not hesitate to let me know.

Best Wishes,

James Kinross

Reviewer: 1

“Although an Analysis article, the tone is sometimes overly colloquial and the prose could be tightened in several places.”

We have attempted to use language that is non-technical, for the reason that most of the readership will not have expertise in this area of cyber security. However, we have addressed this and applied technical language where reasonable and tidied our prose throughout.

“The article is clear in its arguments, and does a strong job outlining the challenge and cost of cyberattacks, with well cited examples. However, it does fall somewhat flat with respect to potential solutions. As such, it may not be particularly engaging for Journal readers, especially those that follow the news closely. That being said, an in-depth discussion of solutions may be too technical and not of sufficient interest to the readers of this Journal.”

There are two main challenges in providing detailed solutions: 1. There is a significant lack of literature to support solutions for cyberattacks in the specific health context. Therefore, we must look to adapt generalisable solutions from other critical sectors which we have included and further signposted. 2. This is a global crisis, and each health system faces its own varying degrees of vulnerability and resource to meet this challenge, framed within local variation in rules and regulations. 3. The recent NHS attack demonstrated that this is to a significant extent a political and policy challenge. We have therefore described these issues and expanded on some of the proposed solutions. We hope that in particular that Figure 2, in which we have adapted the NSCS '10 steps to cyber security' for the health sector is a useful demonstration of solutions. We do however, agree with the final comment the reviewer in that many of the current solutions require significant technical language which may obstruct the reader; we have tried to keep away from this.

Specific Comments

Page 1 lines 14-22 - Please provide citations or references to support your statements

This has been done and phrasing updated.

Page 3 line 36 - Why is there no detailed discussion of the “Integrity” component of the proposed CIA framework

This section has been expanded and “integrity” and “availability” clearly linked as often coming hand-in-hand. We have also referenced these in regards the WannaCry attack, and also in terms of future threats later in the article

Page 4 line 7 - remove “mere”

Done

Page 4 line 9 - remove “got their hospital back.” This reads as too colloquial. Please describe what actually happened

We agree, and we have amended this text.

Page 4 line 33 - Start paragraph with “Although”

We have amended this sentence.

Page 4 line 50-54 - The last sentence in this paragraph is speculative

We agree, and we have provided an example to provide evidence.

Page 5 line 13 - Please provide a reference or citation for this statement

Done.

Page 5 line 37 - Please provide a reference or citation for this statement

Done.

Page 5 line 42 - Please provide a reference or citation for this statement

Done

Page 6 line 33-38 - This is an interesting point. Are there any surveys or qualitative research you could point to in order to better characterize the level of mistrust and the impact on data sharing and research?

We have put this point into clearer context, and included specific references to the recent National Data Guardian Report, and also a specific reference on patient and public views on the security and privacy of eHRs.

Reviewer: 2

Recommendation:

The authors attempt to address a topic of extreme importance and urgency. Many of the points are valid although many are not novel and have already been well covered in the peer reviewed literature dating back to 2014 and before. (please see below).

There has been a recent escalation in the frequency of major attacks on healthcare systems; these outdated reviews written only several years ago as these attacks have used increasingly sophisticated methodologies that are constantly evolving and which readers should be aware of. We have described the most recent Wanna Cry attack for example in the new edit. The reviews listed also focus specifically on the US healthcare system which is very different from many others; we have attempted to make this article as generalisable as possible, however we have included the specific reference raised.

In addition, while the threats are reasonably well covered the emerging controls, standards and resilience methodologies are not covered in this writing but have been covered elsewhere. Utilization of these sources would greatly improve the crispness and utility of the recommendations.

We have extensively updated and re-written the section “*What can healthcare do*” to focus on the future needs, and ways to improve resilience and standards as suggested. Extra references have been added, clear suggestions for future healthcare specific cyber security standards have been included, and Figure 2 has been updated to give a clearer outline of strategies to improve resilience. We have also tightened our discussion around GDPR to also highlight the need for future strategies to deal with this. The “*Key Messages*” have also been updated to reflect these comments.

Lastly, most of the references cited appear to draw more from the lay and trade press versus the peer-reviewed literature that is more common for BMJ articles.

We thank the editor for this comment and we agree that there are many scientific papers written on cyber security. However, we disagree that this topic has been well covered in healthcare. In fact, cybersecurity has been comparatively ignored in the field of patient safety. There is a significant paucity of trials and we were only able to find three systematic reviews of relevance¹⁻³, and there is no level 1a evidence to support interventions. Moreover, much of the literature has been referenced from the lay press, for the simple reason it is not reported in the majority of the medical literature. However, we have now made steps to include more references to established medical text including some of those highlighted.

1. Kruse CS, Frederick B, Jacobson T, et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol Health Care* 2017;25(1):1-10. doi: 10.3233/THC-161263
2. Luna R, Rhine E, Myhra M, et al. Cyber threats to health information systems: A systematic review. *Technol Health Care* 2016;24(1):1-9. doi: 10.3233/THC-151102
3. El Emam K, Jonker E, Arbuckle L, et al. A systematic review of re-identification attacks on health data. *PLoS One* 2011;6(12):e28071. doi: 10.1371/journal.pone.0028071