Network and Information Security Management May 2021 A

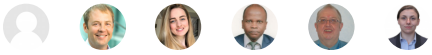
« Collaborative Learning Discussion 1

Charlotte Wilson

Initial Post

14 days ago

8 replies



Last 5 days ago

There are a few key threats / vulnerabilities that stand out when reading the chosen writing Compromising a Medial Mannequin, Healthcare Information Systems and Technology.

One appears to be the lack of focus on improving technology within the medical industry. It was stated that although there is a growing need and dependency on technology within the industry, the healthcare industry is not equipped to deal with a cyber attack (Andel, T. et al., 2015). Unfortunately for many organisations and industries, if investment is not made, they will quickly fall prey to cyber criminals with technology changing every day and the attacks just becoming quicker and easier. To combat this, the obvious answer would be investment; however, I would start to mitigate this threat with user behaviour. It is not always the case of if a breach happens, but when, and although out of date software / lack of secure technologies will definitely aid cyber criminals, improving user behaviour will potentially stop malicious attacks from happening or will ensure the right people are made aware quickly as to mitigate the wider risk.

The other key threat mentioned within the paper was a Denial of Service (DoS) attack. This type of attack is very common and can cause massive issues for organisations (along with reputational and financial damage). A few key ways to mitigate an attack like this would be to ensure monitoring is in place across the network, providing real time visibility for any activity that is an anomaly. The next step would be to ensure an incident response plan is in place (working effectively and reviewed periodically), so that if an attack does happen, actions can be taken quickly to remediate. Another would be ensuring spoofing is prevented as well as it can be. Spoofing can make it more difficult to clearly determine what is legitimate traffic and what is not (Extrahop, N/A).

References

- Andel, T. et al. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth). Available from: file:///home/chronos/u-2c818a963088e2763e3e2dedc0fad6fcf8b6c2ef/MyFiles/Downloads/Compromising%20a%20Medical%20Mannequin.pdf [Accessed 10 May 2021]
- Extrahop (N/A) Denial of Service Attacks and how to prevent them. Available from: https://www.extrahop.co.uk/resources/attacks/dos/ Accessed 10 May 2021]

Reply

8 replies

1 

Post by **Doug Millward**

13 days ago

Feedback

Hi Charlotte
a good post and some good points. As you say technology is not the only answer - people and processes make a difference too. Again a good point about investment - one of my research interests is in the area of "secure by design" and I think a lack of good security design causes a lot of problems.

Reply

2 

Post by **Laura Rivella**

12 days ago

Peer response

Hi Charlotte,

I really enjoyed your take on the article. Since so many have already posted excellent technical solutions, I wanted to take the opportunity to expand on a great point you bring up about the state of cybersecurity in the healthcare industry.

I've been involved in pharma and life sciences in the past years and you are correct in stating that the industry is not equipped to deal with a cybersecurity attack; it wasn't in 2015 and it still isn't today. In the last five years there has been a lot of competition to combine and apply data science, biostatistics and artificial intelligence to try to take market shares away from the competition. However, proper regulation and security standards have not been enforced.

The pandemic has recently caused a - limited - shift in posture, in that a recurrent theme nowadays is the fact that the pharma/healthcare sector is in the sights of cybercriminals due to its role in vaccines and drug development. The trend appears nevertheless to consist of much fearmongering and little action in terms of strengthening of measures or investment in cybersecurity.

Without naming names, even in the consultancy sector, in which we hold a lot of sensitive big pharma client information, we witness weekly - if not daily - attacks and phishing attempts. To this day, no effort to train staff has been made, which could arguably be the most cost-effective solution in this very hypothetical case I'm definitely not involved in.

The only argument one can bring to the table is that it is a sector in which certain kinds of change tend to happen quite slowly.

After more than five years of talks, the Heads of Medicines Agency and the European Medicines Agency held a workshop a few weeks ago on artificial intelligence in medicines regulation, giving a strong signal that regulation is necessary. It will likely take just as many more years for standards of security to be drafted and perhaps enforced.

What is badly needed, and as you rightfully pointed out, is to mitigate these threats with user behavior. In order to do that and educate industry staff, we need to work transversally across sectors and bring cybersecurity expertise in every industry trying to change company cultures from the inside.

Reply

3  Post by **Doug Millward**

12 days ago

feedback

great post Laura. `You raise some very interesting points and I agree that the role of CyberSecurity in medicine/ pharma needs to be urgently reviewed. I see three main areas: staff education so they are aware of the risks; patient education and technology review so that the most up-to-date techniques we apply to IoT devices should be the MINIMUM standard for medical devices.

Reply

4  Post by **David Luvaha**

11 days ago

Peer Response

Regarding incident response plan, the NHS Digital (2020) agrees that timely reaction to security critical incidences was central given the susceptibility of biomedical hardware. Actions to mitigate and eliminate breaches must be well-timed to stop attacks from spreading. Additionally, medical practitioners and clinicians must be engaged to comprehend the effect of any breach and strategies for remediation.

References

NHS Digital (2020) 4.5 Incident response
Available from:
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices
[Accessed 13 May 2021].

Reply

5  Post by **Freya Basey**

9 days ago

Peer Response

Further to Charlotte's point, the medical industry's historic lack of focus on cyber security does not just aid cyber criminals, it also attracts them (ENISA, 2015). Medical industry systems and devices are often seen as an easier target due to poor defences and the widespread use of legacy systems (Tervoort et al., 2020).

Whilst the WannaCry ransomware attack on the National Health Service (NHS) in 2017 was not aimed at unsupported software, the Microsoft Windows vulnerability was present in unsupported versions of the operating system, including Windows XP, and this was still in use in the NHS for critical medical devices (Smart, 2018). Fortunately, Mircrosoft released a Windows XP patch for this vulnerability in May 2017 despite ceasing support for this software in 2014 (Winder, 2020). Lessons learnt from the Wannacry attack include moving away from legacy Windows operating systems but this is still a work in progress after four years.

Another key recommendation from the NHS review was to improve accountability and leadership around cyber security all the way up to Board level. Active support and engagement with cyber security at a senior level is a key driver in ensuring consistent investment in cyber security as well as the establishment of security culture in a top-down fashion (Abraham et al., 2019).

References

Abraham, C., Chatterjee, D. & Sims, R. (2019) Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons 62(4): 539-548.

ENISA (2015) Security and Resilience in eHealth. Available from: **https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services** [Accessed 11 May 2021].

Smart, W. (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack*. Available from: **https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf** [Accessed 15 May 2021].

Tervoort, T., De Oliveira, M., Pieters, W., Van Gelder, P., Olabarriaga, S. & Marquering, H. (2020) Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access* 8: 84352-84361.

Winder, D. (2020) Are old operating systems putting the NHS at risk in 2020? Available from: **https://www.digitalhealth.net/2020/09/are-old-operating-systems-putting-the-nhs-at-risk-in-2020/** [Accessed 15 May 2021].

Reply

6  Post by **Jan Küfner**

7 days ago

peer response

Due to new European wide legislation for medical devices (Medical Device Regulation) and due to compulsory guidelines (MDCG 2019-16) as well as international standards for security specifications (IEC 60601-4-5), it is safe to say, that the level of cyber security will improve for devices sold in the EU in the next years. On the other hand, it is however also likely, that slow adopters will continue to distribute vulnerable devices for some time.

This legislation does have its limitations since it is intended for medical device manufacturers. A ransomware attack, typically done via phishing or using known exploits cannot be prevented by the medical device industry alone. The hospitals, organizations using those devices must improve, too. Many good recommendations to do so such as e.g., operator training, patch management were provided by previous comments already.

References:

European Parliament (2017) Medical Device Regulation, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745&from=DE Accessed on 17.05.2021

European Commission (2019) MDCG 2019-16 - Guidance on Cybersecurity for medical devices, Available at: https://ec.europa.eu/docsroom/documents/41863 Accessed on 17.05.2021

International Electrotechnical Commission (2021) IEC TR 60601-4-5:2021 Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications, Available at: https://webstore.iec.ch/publication/64703 Accessed on 17.05.2021

Reply

Maximum rating: -

7  Post by **Charlotte Wilson**

6 days ago

Summary Post

Within the initial post, two key areas of potential risk were identified regarding the paper in question. The first being a Denial of Service attack, and the other being the lack of focus on improving security controls across the medical industry. In particular, the lack of focus risk was one that was supported well by others among the discussion, in particular with supporting evidence that medical devices are typically targets due to their lack of controls (Basey, F., 2021). This was supported further with note that training of staff to improve general awareness is also not a focus, something of which could benefit the medical industry greatly (Rivella, L., 2021). Both supporting arguments show that it is not only known to those within the industry, but to those seeking easy targets from a cyber criminal perspective. It is clear that more needs to be done.

Alongside mitigation in the form of awareness, other suggested mitigations were provided such as incident response. In particular, the need for timely responses and actions to mitigate and further damage (Luvaha, D., 2021). One other form of potential mitigation suggested was to improve accountability at an Executive / Board level, leading nicely into the previously mentioned solution of education (Basey, F., 2021). Both types of mitigation are key in improving the overall security culture and structure to the medical industry, and both of which require change to the current ways of working.

Overall, all suggestions were in agreement that more needs to be done in this particular area. The more focus provided on people and process, as well as improving technology, the more equipped this industry may become to stopping or recovering quickly from cyber attacks. Even attacks they may not have been directly targeting this industry, can still have an impact and by making small changes, big improvements could be observed. Personally, I believe everything starts with people, with process / technology following after, and I think that is something that all mitigations suggested have in common.

REFERENCES

Basey, F. (2021) Discussion Forum post by Charlotte Wilson, 15 May

Luvaha, D. (2021) Discussion Forum post by Charlotte Wilson, 14 May

Rivella, L. (2021) Discussion Forum post by Charlotte Wilson, 12 May

Reply

8

Post by **Aimalohi Odia**

5 days ago

Peer Response

To effectively mitigate cyber security risk, key decision makers in organisations should make cyber security a priority, organizations must tackle cyber security holistically, this means having technical, operational as well as management controls around assets containing valuable data, for instance, more resources can be invested into cyber security and user behaviour within the organisation can be monitored as mentioned above by Charlotte (Kumar, 2017).

Reference

Kumar, C. J. (2017) 'New Dangers in the New World: Cyber Attacks in the Healthcare Industry', 10(3), p. 15.

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Final Formative Summary and Feedback

NEWER DISCUSSION

Initial Post