Research Methods and Professional Practice March 2022

Home / / My courses/ / RMPP_PCOM7E March 2022 A / / Unit 1 / / Collaborative Learning Discussion 1 /

/ Initial Post /

« Collaborative Learning Discussion 1

Lewle Seneviratne

Initial Post

67 days ago

2 replies

Last 60 days ago

The implantable heart health monitoring device developed by a medical technology startup Corazón and the vulnerability in the wireless connectivity discovered by an independent researcher is considered as a case study for conducting the risk analysis based on the ACM Code of Ethics (CoE) and the BCS Code of Conduct (CoC).

The case study illustrates the application of all the statements from the BCS Code of Conduct (CoC).

The ACM's principle 1.1 (contribute to society and human wellbeing) and BCS's public interest are illustrated by Corazón's charitable work to supply their medical products free or reduced access to patients living below the poverty line. Hence, Corazón's charitable work reflects their increased stewardship towards the quality of life of all people and public health.

While ensuring the safety of the data via encrypted data storage and cryptographic algorithms, led data transfers supports ACM's principle 2.9 (robustly and usably secure system designs); the open bug bounty program exemplifies Corazón's commitment to developing professional knowledge, skills and competence, and the willingness to respect and value alternative viewpoints by accepting honest work criticism, which aligns with BCS's professional competence and integrity, ACM's principle 2.5 (comprehensive evaluations of computer systems). Seeking to improve professional standards through participation in an independent security evaluation, encourage and support the professional development of Corazón's employees and external IT professionals – which uphold the reputation and good standing of BCS.

Further, Corazón's efforts to receive approval from multiple countries' medical device regulation agencies embody the BCS's goal of carrying out professional responsibilities with due care and diligence under the relevant authority's requirements. At the same time, the efforts agree with ACM's principle 3.7 by taking special care of a system that becomes integrated into society's infrastructure.

Reference List

ACM Ethics (2018) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 18 March 2022].

ACM Ethics (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 18 March 2022].

BCS (N.D.)) Code of Conduct for BCS Members. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 18 March 2022].

Reply

Maximum rating: -

2 replies

1

Post by [redacted]

Peer Response

66 days ago

Hi Lewle,

You've chosen a great case study to work with, as it highlights the extent to which Corazón has gone to ensure that their product is not only secure but open and accessible to all (Through their charitable work towards those living below the poverty line). As a result, no notable breaches of either the ACM Code of Ethics or the BCS Code of Conduct were identified (ACM, 2018).

Although Corazón has implemented adequate risk management measures by restricting their developer's work to areas of expertise (ACM, 2018), they have also enhanced this security measure by introducing a "Bug Bounty" scheme. Such schemes are a valuable way of demonstrating an organisations effort towards maintaining a secure application, as they receive the benefit of continuous system scanning and testing (HackerOne, 2021).

If Corazón didn't take the above-mentioned countermeasures, security issues identified in their devices could pose such a risk that they cause fatalities. This would open the door to not only legal action, but from a professional perspective, it would cause breaches in almost all of the ACM/BCS principles.

References:

Association for Computing Machinery. (2018) Case: Medical Implant Risk Analysis. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 20th March 2022].

HackerOne. (2021) Bug Bounty Benefits | Why You Need a Bug Bounty Program. Available from: https://www.hackerone.com/bounty/bug-bounty-benefits-why-you-need-bug-bounty-program [Accessed 20th March 2022].

Reply

2

Post by Lewle Seneviratne

Summary Post

60 days ago

Recognition of health technologies and their role in society is a vital discussion topic.

For this reason, in 2007, the 60th World Health Assembly embraced resolution WHA60.29, covering problems emerging from the improper deployment and use of health technologies and the need to establish emphasis in the selection and management of health technologies (The World Health Organization, 2007).

With the increased use of technologies in healthcare, it is crucial to ensure that technology-driven medical devices are available, accessible, affordable, appropriate, and used safely in society.

Given the criticality of the role, the technology-driven medical devices play in society, having regulated, tested and governed health technology should be coordinated by a designated health technology management in the national governments at all levels of health care.

However, many developing countries and healthcare bodies have to rely mainly on equipment donations due to economic constraints. Although most of these donations are made with good intentions, the outcomes are not always positive if the donations are not properly tested and regulated and if it lacks adequate technical support, leading to many mismanagements in the technology acquisition process (The World Health Organization, 2007). Consequently, effective and efficient technical management of medical devices remains a concern in most low-income countries and middle-income countries as well as healthcare bodies due to bias from a legal and compliance standpoint despite the existence of dedicated, responsible units at the national level.

Thus, this raises the critical question: Who should regulate technologies-driven health equipment? In Corazón's case study, Corazón's efforts to receive approval from multiple countries' medical device regulatory agencies should be vetted carefully, understanding whether these are unbiased approvals or based approvals led by the donations of implantable heart health monitoring devices.

Therefore, simply assuming that Corazón embodies the BCS's goal of carrying out professional responsibilities with due care and diligence under the relevant authority's requirements may not be accurate without in-depth insight into the context.

However, as Kieron also emphasises in the peer posting, the introduction of a "Bug Bounty" scheme demonstrate Corazón's effort to maintain a secure application and the willingness to respect and value alternative viewpoints by accepting honest work criticism.

Nevertheless, in 2016 independent security research group MedSec attempted to attack several St. Jude Medical devices, released partial information about the vulnerabilities to the public, and made significant profits from the venture by working with Muddy Waters. On the other hand, MedSec's concerns regarding St Jude Medical's foot-dragging were not entirely misplaced as there has been virtually no improvement unless there is a major financial or reputational impact in doing so for technologies-driven health equipment technology manufacturers (Macnish & Ham, 2020).

Thus, MedSec/Muddy Waters/St Jude Medical case has two-fold should cybersecurity researchers be safeguarded from legal action such as the effort to sue MedSec by St Jude? How could we ensure that technologies-driven health equipment takes a severe step towards taking actions to test the flaws highlighted by independent researchers rather than foot-dragging with no improvement unless there is a significant financial or reputational impact in doing so?

Here MedSec/Muddy Waters/St Jude Medical case raises another critical question: Would be introducing a "Bug Bounty" be enough to evaluate Corazón's effort to align with BCS's professional competence and integrity? Would it be worthwhile to evaluate the processes undertaken by Corazón to evaluate vulnerability flaws highlighted through the "Bug Bounty" scheme before evaluating its Ethics and Professional Conduct?

References

ACM Ethics (2018) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 18 March 2022].

ACM Ethics (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 18 March 2022].

BCS (N.D.)) Code of Conduct for BCS Members. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 18 March 2022].

Macnish, K. & Ham J. V. (2020) Ethics in cybersecurity research and practice. Technology in Society 63. DOI: 10.1016/j.techsoc.2020.101382.

The World Health Organization (2007) The impact of algorithms for online content filtering or moderation. Available from: https://www.who.int/medical_devices/management_use/3_4.pdf [Accessed 24 March 2022].

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post

NEWER DISCUSSION

Summary Post