Elgabry *Crime Science* (2023) 12:3
https://doi.org/10.1186/s40163-023-00181-8

Crime Science

SHORT CONTRIBUTION

Open Access

Towards cyber-biosecurity by design: an experimental approach to Internet-of-Medical-Things design and development

Mariam Elgabry[1,2,3*]

Abstract

The introduction of the internet and the proliferation of internet-connected devices (IoT) enabled knowledge sharing, connectivity and global communications. At the same time, these technologies generated a crime harvest as security was overlooked. The Internet-of-Medical-Things (IoMT) generates biological information and is transforming healthcare through the introduction of internet-connected medical-grade devices that are integrated with wider-scale health networks to improve patients' health. Many innovative ideas arise from academia; however, there is a lack of support in medical device regulation. The implementation of the current regulatory framework is limited to security risk assessment and guidance. Unfortunately, premarket risk-management requirements of current regulation do not include crime risks and a more predictive approach could help fill this gap. Crime science, or the perspective of crime as an event that can be influenced directly by its immediate environment, may encourage the biotechnology industry to design-in security and crime out. In this article, I provide a point of view of an early career researcher and medical device developer navigating the medical device regulatory pathway for the first time. I narrow the focus of this article to an assessment that is specific to current UK provisions and acknowledge the limited scope. In response to the ongoing changes in the current regulatory framework of the UK, I propose a new secure by design mechanism that can be employed by early career developers earlier in the development process of a product. Such a model can be used to systematically consider security design in devices and to understand and address potential crime risks ahead of their widespread use.

Keywords Crime science, Crime harvest, Internet-of-Medical-Things, Medical devices, Internet-of-Things, Medical device regulation

The Internet-of-Medical-Things and crime opportunity

The introduction of the internet and the proliferation of internet-connected devices (IoT) enabled knowledge sharing, connectivity and global communications. At the same time, these technologies generated emerging crime opportunities—a "crime harvest" (Pease, 1997)—as security was overlooked (Blythe and Johnson, 2021). A systematic review of 114 synthesized studies discovered that several consumer IoT devices such as smart

*Correspondence:
Mariam Elgabry
Mariam@bronic.co; M.elgabry.17@alumni.ucl.ac.uk
[1] DAWES Centre for Future Crime at UCL, Jill Dando Institute for Security and Crime Science, 35 Tavistock Square, London WC1H 9EZ, UK
[2] UCL Biochemical Engineering, Bernard Katz, London WC1E 6BT, UK
[3] Bronic Ltd, 28 Belsize Avenue, London N13 4TJ, UK

meters and smart locks enabled a wide range of crime types from burglary to stalking crimes (Johnson et al, 2020). Even more worrisome may be the security implications of connected devices that do not collect information about household appliances from connected TVs or fridges, but that collect health data. Medical devices are products (instrument, apparatus, machine, implant, software or related article) intended to be used with a specific medical purpose(s) of diagnosis, prevention, monitoring, treatment or alleviation of disease (WHO, 2022). These generate biological information and are transforming healthcare through the introduction of the Internet-of-Medical-Things (IoMT), internet-connected medical-grade devices that are integrated to wider-scale health networks in order to improve patients' health (e.g. remote patient monitoring) (Bhatia et al., 2021; Terry, 2016). The transformation of healthcare has been ongoing. In the United Kingdom, for example, the National Health Service (NHS) recently launched its national NHS App Library, installing WiFi across the NHS estate, enabling citizens to transact with the NHS, all from their computer or smart phone (NHS, 2019). The global COVID19 pandemic has also arguably accelerated this process as IoMT devices are expedited to the market in response, to try and address the unmet need of remote patient monitoring to improve patients' medical experience. Albeit a testimony to a rapid response, there is risk for unintended consequences if security is overlooked.

As IoMT devices collect information about patients and their health, it is vital that they are secure as they do not only gather information but are able to affect patient's health if their security is compromised. When security is overlooked, these vulnerabilities create opportunities for crimes if the data can be stolen, as occurred with the National Health Service (NHS) WannaCry ransomware attack (O'Dowd, 2017). In addition to the stolen encrypted data and files, the ransomware attack also impaired the functionality of the NHS in England, blocking and preventing staff from accessing patient data and critical services (Ghafur et al, 2019) and causing direct harm. Two examples of direct harm caused by interfering with health outcomes through hacking are described by Applegate (2013) and Li et al. (2011). Applegate exposed a vulnerability in a pacemaker that gave unauthorized access to and control of the device, allowing a third party to deliver an unwarranted shock through a pacemaker via wireless transmission. Li et al., 2011 disclosed vulnerabilities found in insulin pumps used to deliver regular insulin throughout the day, which could potentially be exploited to alter the intended therapy and administer an overdose to the patient remotely. While these two examples were security vulnerabilities demonstrated in a laboratory and were not intentionally exploited to harm, they could be considered criminal negligence (Elgabry et al., 2022; Wellington, 2013). During product development, it is not unusual that insufficient attention is given to the crime implications of new products entering the market, giving rise to "crime harvests" or emerging crime opportunities (Pease, 1997). Criminals are early adopters of technology and thus exploit these vulnerabilities before they are addressed. In the UK, The Department for Digital, Culture, Media and Sport (DCMS) launched a code of practice to encourage manufacturers to improve the security standards of consumer IoT devices (IoT Code of Practice & DCMS, 2018). However, this is currently dependent upon trusting responsible manufacturers to implement it. Currently, this same trust exists in IoMT devices since premarket risk-management requirements of current regulation do not explicitly include crime risks.

The Internet-of-Medical-Things and current UK regulation

IoMT devices are usually subject to prescribed standards overseen by a relevant government agency. In the UK, medical devices are regulated under the Medical Devices Regulations 2002 (UK MDR, 2002),[1] which implement existing European Union (EU) medical devices directives into UK law via the Medicines and Healthcare products Regulatory Agency (MHRA) (Singh, 2022). This agency also provides standards to ensure security, safety and effectiveness of the devices. Devices are classified by risk comprising different requirements. Manufacturers of low-risk products (medical device classification Class I, which includes bandages, handheld surgical instruments) can provide a self-certification, whilst for products of higher risk classification (Intermediate risk Classes IIa, IIb such as computed tomography (CT) scan and highest risk Class III, which include devices for sustaining life such as pacemakers), a conformity assessment is required. A sample of the risk assessment provided by the manufacturer is then checked by a notified body such as the British Standards Institution (BSI). To indicate compliance with EU legislation, IoMT devices sold within the UK required CE marking under the EU Medical Devices Directive (MDD) (Directive 93/42/EEC) (European Council Directive 1993) (formally Medical Devices Regulation (MDR) 2017/745) (European Union 2017).

The UK has so far followed EU regulation; however since exiting the EU on 31 January 2020, it is requiring new arrangements to come into place for the continued regulation of medical devices to ensure that they are safe and effective within the UK market (Department

[1] The Medical Devices Regulations (2002) https://www.legislation.gov.uk/uksi/2002/618/contents/made.

for Business, Energy & Industrial Strategy, 2021). To respond to the opportunities and challenges arising from leaving the EU, the UK has prioritized innovation, and is undergoing regulatory reform to support this as a central part of the UK Government's strategy (Department for Business, Energy & Industrial Strategy, 2021). On 1 January 2021 the UK Conformity Assessment (UKCA)[2] mark came into force and is required for certain products that are placed on the Great Britain (England, Wales and Scotland) market. From 1 July 2023, the previously accepted CE mark will no longer accept new products placed on the market in Great Britain (Han et al., 2022). The contents of the new legislation to be enforced in the UK in July 2023 are not yet known, but may have similarities to the EU MDR (Kwong et al., 2021). For example, for class I devices that can be 'self-certified' by a manufacturer, the self-declaration of conformity for UKCA marking is expected to be the same as for CE marking (Almilaji et al., 2022). For other types of devices such as implanted devices, the recent consultation in November 2021 on the future regulation of medical devices in the UK indicated an appetite for further requirements such as national device registries for the collecting and sharing of information (Jeffery, 2022). As the transition to the UK reform continues, some manufacturers are still operating under the previous regulations, which can also introduce opportunities for crime, error and/or insecurity.

At present information is fragmented across different standards (e.g., IEC standards 62,304 or 80,001–5-1on software development and ISO 14971),[3,4,5] creating a lot of uncertainty for manufacturers of IoMT devices around the identification of the appropriate standards associated with the regulatory requirements. This shortcoming may have a detrimental effect on medical device innovation as start-ups and SMEs will have difficulty overcoming regulatory uncertainty with their lack of in-house expertise (Ben-Menahem et al., 2020; Granlundet al., 2021). Regulating devices is challenging as IoMT applications are diverse, including both hardware and software applications (GHTF, 2005). To illustrate, IoMT includes but is not limited to artificial intelligence as a medical device (Beckers et al., 2021), thermometers, artificial hearts (Slepian et al., 2013), stents, Sonogram machines, X-ray machines, stethoscopes (e.g., Astono et al., 2017), and wheelchairs (e.g., Cooper, 2006). Consequently, this challenge may lead to crime exponentiation, a condition whereby "advancements in technology lead to evolutions in crime that outpace our ability to conceptualize and respond to them" (Topalli & Nikolovska, 2020).

Many innovative ideas arise from academia; however there is a lack of support in Medical Device regulation (Hendricusdottir et al., 2021). Hendricusdottir et al. conducted a systematic search of information found online that provided support for universities in medical device regulation found that 55% of the selected universities in the UK did not provide any. As a result of these findings, the authors suggested that the early phases of research and development will need an increase in support for regulatory strategies to yield a better translation of technologies into clinical care. The implementation of the current regulatory framework often is limited to a security risk assessment and guidance, as opposed to active security testing, and requires more (specialized) auditing. Current risk-based and compliance approaches to the security of IoMT devices are limited and a more predictive approach could help fill these gaps. Unfortunately, premarket risk-management requirements of current regulation do not include crime risks.

The need for "Cyber-biosecurity by design"

Although manufacturers consider the security of a device for the regulatory requirements, these do not explicitly include crime risks that can be assessed throughout the design process as a proactive approach. Moreover, conformity can only be shown in a "complete" and final device. A manufacturer cannot declare or prove conformity for a theoretical device—as extensive information is needed, for example, the manufacturing procedures, instructions of use, labelling and packaging, to name a few. While notified bodies encourage manufacturers to schedule formal meetings to discuss their device and provide comments, early career researchers and medical device developers do not have easy access to such consulting (Maresova et al., 2020). As the UK steers it own course in the future, balancing the regulation of medical devices such that dangerous or unintentionally harmful devices do not enter the market while not being too restrictive for truly innovative solutions (Jeffery, 2022).

Researcher and innovator unfamiliarity with medical device regulations can often be a barrier to translating technology into a clinical setting (Kwong et al., 2021). In response to the ongoing changes in the current regulatory framework of the UK, and from the point of view of an early career researcher and medical device developer navigating the medical device regulatory pathway for the

[2] UK Conformity Assessment [Internet]. GOV.UK. 2021 [cited 2021 Jul 2]. Available from: https://www.gov.uk/guidance/uk-conformity-assessment.

[3] International Electrotechnical Commission (IEC) Medical device software—Software life cycle processes (62,304:2006) https://www.iso.org/standard/38421.html.

[4] International Electrotechnical Commission (IEC) Health software and health IT systems safety, effectiveness and security—Part 5–1: Security—Activities in the product life cycle (81,001–5-1:2021) https://www.iso.org/standard/76097.html.

[5] International Organization for Standardization (ISO) Application of risk management to medical devices (14,971), https://www.iso.org/standard/72704.html.

first time, I propose a mechanism which allows manufacturers and/or developers to take an experimental approach to their device design. Hosting a hackathon with an embedded Delphi process, could be deployed at institutions and/or manufacturing facilities. "Hackathon" refers to an event that brings domain experts to collaborate intensively on a project (Tucker et al., 2018). The term "hack" here has a positive meaning and is defined as the "finding [of] unintended or overlooked uses" and "applying them in new and inventive ways to solve a problem—whatever it might be" (Erickson, 2008, pg. 1). The term hackathon comes from the combination of the words hack and marathon to highlight the focused effort such as that of a marathon of finding a solution to a given problem (Komssi et al., 2015). Although relatively new, the hackathon model has been useful to various applications such as medical technology innovation (e.g., DePasse et al., 2014). The Delphi process is an established forecasting approach that at its most basic form involves several rounds of surveys with experts, who are questioned individually, to eventually reach a "consensus" (Dalkey & Helmer, 1963; Linstone & Turoff, 1975; Turoff, 1970). A hyBrid hAcKathon dElphi (BAKE) framework (Elgabry, 2021)—or a similar framework—that couples the scenario building (of the Delphi process) and the prototyping (of the hackathon) can be used as a mechanism to systematically consider security design in devices and to understand cybersecurity compliance issues—ahead of their widespread use. The Delphi process within the BAKE can help answer key questions regarding the Internet-of-Medical-Things, including what areas might be misused and security features considered necessary. The benefits of the prototyping through the hackathon model are proactive and continuous penetration testing to search and find security weaknesses early. While there may be such iterative design and testing processes applied in, for example, the software development of medical devices, the BAKE framework can be applied to capture highly challenging threats and risks within the whole cyber-physical device system—attending to the cyber-biosecurity of the device. As an early career researcher and medical device developer with no in-house expertise for security compliance, I found it helpful to fill this knowledge gap through a proactive crime risk assessment that was engaging in "thinking thief" during the ideation and materialization of the medical device I was developing—as opposed to fitting security requirements retrospectively. Today, security is dynamic—especially as systems and devices are increasingly more integrated—and therefore testing cannot be static (Yousefnezhad et al., 2020). By adopting an experimental approach through hosting a hackathon with an embedded Delphi process, (bio)secure by design can be prompted earlier in the product development life cycle of any medical technology.

Conclusion

The Internet-of-Medical-Things (IoMT) is transforming healthcare through the introduction of internet-connected medical-grade devices that are integrated to wider-scale health networks to improve patients' health. Unfortunately, crime implications of new medical products entering the market are often overlooked during product development in the current regulatory framework. Despite new medical device regulation, uncertainty in the security conformity of the IoMT urges the need for "CyberBiosecurity by design". A hyBrid hAcKathon dElphi (BAKE) framework—or a similar framework—can be introduced as an experimental approach for IoMT design and development. This is a forward-thinking mechanism that can systematically consider security design in devices ahead of their widespread use during design phase of a product lifecycle, and while, prototyping. With the adoption of an experimental approach by researchers and innovators, novel risks and threats to cyber-biosecurity can be identified early to reduce the likelihood of an unintended crime harvest occurring in the future.

Acknowledgements

The author would like to acknowledge the EPSRC and the Dawes Centre for Future Crimes at UCL that funded and supported the research. The author would also like to acknowledge Christoph Kiesselbach (Partner at Schrack & Partner, GER) who provided a valuable contribution to the work with his expertise in medical device and medicinal product regulatory affairs and quality management.

Author contributions

M.E. wrote the manuscript. The author read and approved the final manuscript.

Funding

This work was supported by the EPSRC and Dawes Centre for Future crimes at UCL, grant reference number [1918475]. The views expressed are those of the author(s) and not necessarily those of the EPSRC or Department of Security and crime Science, Jill Dando Institute. For more information and current projects researched at the Jill Dando Institute and the Dawes Centre for Future Crimes, follow the link https://www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime#Research.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The author declares that they have no competing interests.

Received: 11 April 2022 Accepted: 2 February 2023
Published online: 17 February 2023

References

Almilaji, O., Engen, V., Snook, J., & Docherty, S. (2022). The development of a clinical decision-support web-based tool for predicting the risk of gastrointestinal cancer in iron deficiency anaemia—the IDIOM app. *Digital, 2*(1), 104–119.

Applegate, S. D. (2013). The dawn of kinetic cyber. In *2013 5th international conference on cyber conflict (CYCON 2013)* (pp. 1–15). IEEE.
Astono, J., Purwanto, A., & Agustika, D. K. (2017). The improvement of phonocardiograph signal (PCG) representation through the electronic stethoscope. In: *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* (pp. 1–5). IEEE.
Beckers, R., Kwade, Z., & Zanca, F. (2021). The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. *Physica Medica, 83*, 1–8.
Ben-Menahem, S. M., Nistor-Gallo, R., Macia, G., von Krogh, G., & Goldhahn, J. (2020). How the new European regulation on medical devices will affect innovation. *Nature Biomedical Engineering, 4*(6), 585–590.
Bhatia, R. S., Shojania, K. G., & Levinson, W. (2021). Cost of contact: Redesigning healthcare in the age of COVID. *BMJ Quality & Safety, 30*(3), 236–239.
Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal, 34*(1), 97–125.
Cooper, R. A. (2006). Wheelchair standards: It's all about quality assurance and evidence-based practice. *The Journal of Spinal Cord Medicine, 29*(2), 93.
Department for Business, Energy & Industrial Strategy (2021). Life science sector data, 2020. GOV.UK. Retrieved 26 July 2021, from https://www.gov.uk/government/publications/life-science-sector-data-2020.
Department for Digital, Culture, Media and Sport DCMS (2018) "Code of Practice for Consumer IOT Security." GOV.UK. 2018, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.
Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458–467.
DePasse, J. W., Carroll, R., Ippolito, A., Yost, A., Chu, Z., & Olson, K. R. (2014). Less noise, more hacking: How to deploy principles from MIT's hacking medicine to accelerate health care. *International Journal of Technology Assessment in Health Care, 30*(3), 260–264.
Elgabry, M. (2021) National machinery: Red-teaming approach written evidence. *UK Parliament Joint Committee on National Security and Machinery*, UK Parliament.
Elgabry, M., Nesbeth, D., & Johnson, S. (2022). The future of biotechnology crime: A parallel delphi study with non-traditional experts. *Futures, 141*, 102970.
Erickson, J. (2008). *Hacking: the art of exploitation*. No starch press.
European Council Directive. (1993). European council directive 93/42/EEC of 14 June 1993 concerning medical devices. *Official Journal of European, 169*, 1–43.
European union. (2017). Regulations (EU) 2017/745 of the European parliament and of the council of 5 April 2017 on medical devices. *Official Journal European Union., 117*, 1–175.
Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: The UK National Health Service as a case study. *The Lancet Digital Health, 1*(1), e10–e12.
GHTF Study Group (2005) Information document concerning the definition of the term "medical device". The global harmonization task force; May. http://www.imdrf.org/docs/ghtf/final/sg1/technical-docs/ghtf-sg1-n29r16-2005-definition-medical-device-050520.pdf.
Granlund, T., Vedenpää, J., Stirbu, V., & Mikkonen, T. (2021). On medical device cybersecurity compliance in EU. In: *2021 IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH)*. IEEE. (pp. 20–23).
Han, J. E. D., Ibrahim, H., Aiyegbusi, O. L., Liu, X., Marston, E., Denniston, A. K., & Calvert, M. J. (2022). Opportunities and risks of UK medical device reform. *Therapeutic Innovation & Regulatory Science*. https://doi.org/10.1007/s43441-022-00394-0
Hendricusdottir, R., Hussain, A., Milnthorpe, W., & Bergmann, J. H. (2021). Lack of support in medical device regulation within academia. *Prosthesis., 3*(1), 1–8. https://doi.org/10.3390/prosthesis3010001
Jeffery, S. (2022). The regulation of medical devices in the UK: Recent changes. *British Journal of Nursing, 31*(4), S4–S6.
Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLoS ONE, 15*(1), e0227800.
Komssi, M., Pichlis, D., Raatikainen, M., Kindstrom, K., & Jarvinen, J. (2015). What are Hackathons for? *IEEE Software, 32*(5), 60–67. https://doi.org/10.1109/ms.2014.78
Kwong, M. T., Stell, D., & Akinluyi, E. (2021). Medical device regulation from a health service provider's perspective. *Prosthesis, 3*(3), 261–266. https://doi.org/10.3390/prosthesis3030025
Linstone, H. A., & Turoff, M. (Eds.). (1975). *The delphi method* (pp. 3–12). Addison-Wesley.
Maresova, P., Hajek, L., Krejcar, O., Storek, M., & Kuca, K. (2020). New regulations on medical devices in Europe: Are they an opportunity for growth? *Administrative Sciences, 10*(1), 16.
NHS LongTerm Plan (2019) Retrieved 13 September 2022, from https://www.longtermplan.nhs.uk/publication/nhs-long-term-plan/.
O'Dowd, A. (2017). NHS patient data security is to be tightened after cyberattack. *BMJ: British Medical Journal (online)*. https://doi.org/10.1136/bmj.j3412
Pease, K. (1997). Predicting the future: The roles of routine activity and rational choice theory. In G. Newman, R. V. Clarke, & S. G. Shoham (Eds.), *Rational choice and situational crime prevention: Theoretical foundations* (p. 233). Dartmouth.
Singh, K. (2022). Device regulations of other countries. In P. Srinivasan, T. Shanmugam, P. Thangaraju, N. Palani, & T. Sampath (Eds.), *Medical device guidelines and regulations handbook* (pp. 347–376). Springer.
Slepian, M. J., Alemu, Y., Soares, J. S., Smith, R. G., Einav, S., & Bluestein, D. (2013). The Syncardia™ total artificial heart: In vivo, in vitro, and computational modeling studies. *Journal of Biomechanics, 46*(2), 266–275.
Terry, N. P. (2016). Will the internet of things transform healthcare. *Vanderbilt Journal of Entertainment and Technology Law, 19*, 327.
Topalli, V., & Nikolovska, M. (2020). The future of crime: How crime exponentiation will change our field. *The Criminologist, 45*(3), 1–8.
Turoff, M. (1970). The design of a policy Delphi. *Technological Forecasting and Social Change, 2*(2), 149–171.
Wellington, K. (2013). Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions. *Santa Clara High Technology Law Journal, 30*, 139.
World Health Organization (2022) Retrieved 13 September 2022, from https://www.who.int/health-topics/medical-devices#tab=tab_1.
Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications, 171*, 102779.

Publisher's Note