Do You Speak Cyber?
Talking Security with Developers of Health Systems and Devices

Charles Weir | Lancaster University
Anna Dyson | Lancaster University
Dan Prince | Lancaster University

Security and privacy concerns are vital in software for health-related applications. Yet often their development teams in small companies have little professional security support. To work effectively with them we should accept the complexity of their decision-making, create stories as a basis for discussion, and use different jargon from cyber-professionals.

Security and privacy are vital software properties, and critical in health-related devices and applications [40]. Yet many cyber security practices can be poorly suited to modern agile development approaches and to systems involving many internet-accessible components [3], such as Health Internet of Things (HIoT) systems [8]. Further, the cost and lack of availability of cyber security professionals makes it unrealistic to have dedicated cyber security support in small companies. Instead, responsibility for security and privacy is typically delegated to non-security-specialist developers. Lacking support from cybersecurity professionals, in small to medium companies such developers frequently turn to industry-based training and open sources for support and guidance materials [1].

Consider such small company HIoT developers—meaning everyone responsible for development, including testers and decision-makers. For them, security and privacy are just two aspects amongst many for the product they are developing. The teams thus have limited time available to devote to learning about them. Any guidance or advice must use developers' language and mesh with their existing procedures and operations, otherwise it risks being ignored, misunderstood or devalued. To make guidance and support usable for developer teams therefore requires knowledge of the language they use to discuss cybersecurity. It also requires an understanding of how their cybersecurity decisions are made. Yet, currently that knowledge and understanding are anecdotal at best, and frequently non-existent. If we, as academics and security specialists, are to work with development teams to improve cyber security practice in heath and health-related devices, we must learn to talk the developer's own language: to **speak their dialect of cybersecurity**.

The goal of this article, therefore, is to explore, for the important domain of Health Internet of Things software, how small company development teams discuss and decide on security and privacy issues, to support training and interventions by academics and security specialists.

To that end, the authors used a qualitative approach, interviewing 20 senior software professionals in small companies creating health-related devices and services. The research gathered data using open question interviews to explore the topics in two different ways. First was evaluation of four predictions that we made based on prior work. Second was open exploration of development teams' decision making and language relating to security and privacy. Thematic analysis of the transcribed interview data produced a nuanced picture of security and privacy practice in the participants' teams.

The Research Process

Figure 1 shows the stages in the research process. Rounded rectangles show activities; rectangles, artefacts; and arrows, the resulting contributions. We minimized bias through diversity in the participant pool; by piloting the survey instrument; with reviewing codes; and by using dual coding—even for open coding. The stages are highlighted in the following descriptions.

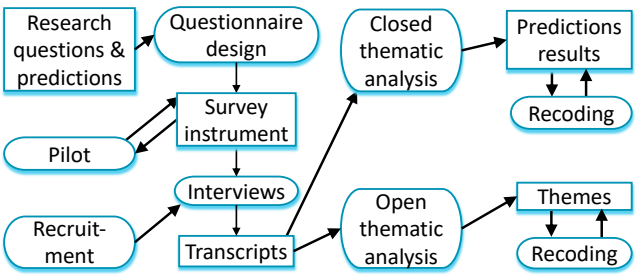

Figure 1: Research Process

The two **research questions** the research sought to explore are:

RQ1. How do independent HIoT software development teams describe and discuss security and privacy?

RQ2. How do independent HIoT software development teams make decisions about security and privacy?

From these questions, we identified **predictions** based on prior work [10] and our experience of working with development teams. Two predictions related to RQ1:

PR1. There is inconsistency between developers' and stakeholders' understanding of key concepts, and that of security experts

PR2. Developers use 'War stories'—spoken tales of relevant incidents—to communicate about security and privacy issues

Two further predictions related to RQ2:

PR3. Development teams do not analyse threats and the risks they pose in agile development processes related to Health IoT

PR4. The security and privacy of the product or service is not considered a saleable aspect

Data Collection

We designed a **survey instrument** of 32 open questions, to probe the predictions and elicit qualitative information related to language and decision-making approaches (RQ1 and RQ2). The questions included asking participants to sketch their understanding to clarify concepts.

We **piloted** the survey with two colleagues experienced in commercial software design (though not in the Health IoT domain) to check timing and comprehensibility. One question was added, and five questions were categorized as optional to keep the survey to time. The final version of the **survey instrument** is publicly available[1].

To **recruit** participants, we used three sources: contacts, of the authors and from the university business network; open advertisement such as email newsletters and social; and cold calling to Health IoT companies. To identify when 'thematic saturation' [2] was reached, analysis was conducted in parallel with interviews.

Interviews were online using Microsoft Teams, which provides both recording and automated transcription. Transcripts were anonymized, corrected, and imported[2] into the Qualitative Data Analysis tool NVivo.

Data Analysis

The thematic analysis followed the six-stage process established by Braun and Clarke [4]. This involves:

1. familiarizing yourself with the dataset by reading transcripts and listening to recordings of interviews;
2. an initial analysis of the dataset through coding, giving labels to the excerpts and concepts found;
3. exploring your codes for emergent themes, finding patterns across the dataset;
4. refining and reviewing those themes against the dataset;
5. finalizing and naming themes; and
6. writing up the results of your analysis.

We used combinations of open coding (emergent, inductive), and closed coding (with predefining codes) to generate meaningful analysis [4]. For example, the closed code 'definition of security' provided many definitions; to summarize them, we open coded 'definition categories' within the coded text. And we analyzed the emergent open code 'decisions and prioritization' using closed coding, into categories 'formal', 'informal' and 'none'. We also used pairs of codes to capture magnitude. For example, every statement coded to 'story use' (PR2) had an additional category code 'never', 'occasional' or 'frequent'.

To analyze the participants' sketches, an independent researcher created text descriptions of each. These and the participants' verbal descriptions provided text for the thematic analysis [6].

We used dual coding throughout the closed coding process: two researchers coded all the data independently, meeting regularly to compare notes and coding. We also used dual coding to categorize attributes of the participants, such as target customer, product category and company size. Following the initial coding round, the two researchers doing the coding then then discussed their differences and recoded accordingly.

To conduct the inductive **open thematic coding,** we created new codes during the coding process to express new concepts as they were discovered. Given that decisions on what is important are subjective, we used the unusual 'reflexive' approach of dual open coding [5]. Our approach was iterative: in each iteration two coders agreed on three or so interview transcripts to code, then each independently open coded those transcripts. They then met to compare the coding, agree on a synthesis of the code sets, and decide on any changes to the coding approach. After this, they continued with the next iteration.

Following the initial coding of all of the interviews, we returned to **recode** all the previously coded transcripts. This

[1] https://github.com/SecurityEssentials/DoYouSpeakCyber

[2] Our tool to convert transcript formats is available at https://securityessentials.github.io/Teams2NVivo/

Figure 2: Word Cloud and Participant Usage of Key Concepts. NICCS glossary terms are in black

found further instances that fitted each code and fixed some erroneous coding.

To transition from codes to themes, using Braun and Clarke's approach [4], we clustered the codes by unifying features into themes. We then reviewed all themes against the codes to ensure the completeness of the set. Codes that did not fit any possible themes were omitted [4]. We then gave names to the themes, and wrote up the results.

The research was approved by the Lancaster University FST Ethics Committee.

Results and Prediction Evaluation

We recruited and interviewed 20 participants, as follows:

- 12 interviewees were at C-Level or Vice President; the rest were senior development staff.
- Their professional experience ranged from 3 to 40 years (median 20, interquartile range 17).
- All worked on health-related products. 15 were currently working, or had recently worked, on IoT-related products.
- 14 worked for 'small' organizations of less than 500 staff, with 6 'medium' ones up to 10,000.
- 17 were United Kingdom-based, with others in the Netherlands, India and Denmark.

Participants' work provided remote monitoring (5 interviewees), health service administration (4), software components (4), patient devices (3), consumer self-care (3) and artificial intelligence-based diagnosis (1).

The interviews generated a total of 21.5 hours of audio. Some participants were reluctant to draw, and only 12 participants' drawings were captured.

Cyber Language Use

It seems reasonable to assume that people working together in a development team will share a technical vocabulary and use that in discussion. To explore PR1 (*inconsistency in understanding of key concepts*), therefore, we analyzed the transcripts using open coding to identify key terms used by participants. Next, we added terms from the NICCS glossary of 235 common cybersecurity words and phrases [7]. Finally, we assessed the interview transcripts for the participants' usage of the combined set, being careful to exclude semantically different uses (such as 'trustworthy system' or 'hospital trust' for 'trust').

Figure 2 shows a word cloud of the results. Word sizes denote the number of participants who used each term; black terms are those defined in the NICCS glossary; red terms are those unique to the interviewees. Terms mentioned by only one person are omitted, as are concepts included in the questions (such as 'security', 'privacy').

As shown, where common concepts were used, many of them were the standard ones used by cybersecurity practitioners. Note, however, that most were little used: even 'threat', for example, occurred in only 11 interviews. Moreover, where the words were standard, the meanings were not always so: four participants used 'a risk' to mean 'a threat', for example.

Two groups of non-standard terms appeared often in the discussions:

Trust refers to stakeholders' trust of the systems. The related terms 'confidence' and 'reputation' tended to be found in the same context.

Safety was vital for the many practitioners working with safety standards. 'Certification' and 'governance' requirements were often related to patient safety.

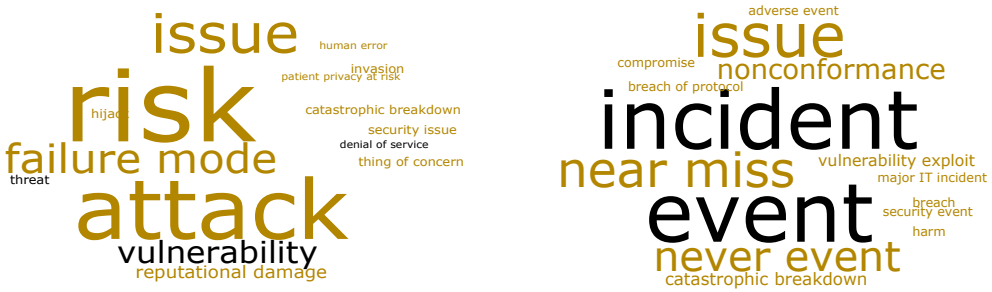

Figure 3: Terms used for Threat (left) and for Incident (right); terms used with cyber-expert meaning are in black

Next, we looked at participants' **discussion around four key concepts.** These concepts were:

Threat: a potential cybersecurity-related problem,
Threat actor: an individual who might deliberately or accidentally trigger such a problem,
Incident: an occurrence of such a problem, and
Victim: people or organizations adversely affected by an incident.

We found that two of these concepts, 'threat actor' and 'victim' rarely had a generic term. Instead, interviewees named specific roles: 'criminal', 'hacker', 'user', 'nation state' for the threat actor; and 'shareholder', 'company', 'user', or 'patient' for the victim. Indeed, seven interviewees stated that their most likely and damaging 'threat actors' were the professional users of the systems.

We found most of the participants did identify terms for 'threat' and 'incident', as shown in Figure 3. Here, colors and word sizes reflect the use of each term *with those specific meanings.* Usage was not at all consistent between participants; the largest words in each cloud represent only 4 participant uses.

Lastly, we asked participants to **define 'security' and 'privacy'**. Almost all participants explained 'security' in terms of the aspects of cybersecurity most relevant to their own products. They defined security in one of three ways: technical features provided by the product implementation; possible and implied harms prevented; or a desired social or commercial outcome. The top part of Table 1 shows examples and how many participants used each one.

Unsurprisingly given the sensitivity of health information, 'privacy' was an important concern for many of the participants. As with 'security', the bottom part of Table 1 shows several different approaches to defining it. Many specified the outcomes achieved by successful privacy; others expressed it in terms of compliance, referring to standards such as GDPR; and one participant did not use the term at all.

Use of Stories

The analysis of prediction PR2, (*developers use stories*), found that pure 'war stories', in the limited sense of "how I diagnosed and fixed a cyber issue" were relatively rare. But 'stories', representing cybersecurity knowledge with an ad hominem example, were common.

Indeed, many participants used stories in answering questions. So, we also analyzed their discussions on other topics, finding that 17 of the 20 participants used stories in this way. Here is one example:

> *A guy I worked with used to defend a lot of people in court against phantom withdrawals. And his argument was this. You're saying my client withdrew £50 in this cash point. He said he doesn't, so I want to*

Table 1: How Participants Defined Security and Privacy

Approach	**Security descriptions**	**Used by**
Harms prevented	*Protecting the patient's identity (Product Manager)*	8
Technical features	*Passwords, … screen timeouts… and different levels of access to the application (Developer)*	5
Desired outcome	*We have to keep our patient feeling … safe … and secure (Entrepreneur)*	7
Approach	**Privacy descriptions**	**Used by**
Outcome	*It's supposed to be near impossible to track back data to an individual, so it's anonymous as much as it can be. (Developer)* *Enabling the data owner to decide who and what data a third party has access to (Team Lead)*	14
Compliance	*PII personal, identifiable information: GDPR, HIPAA compliance. (Vice President)*	5
Not used	*Privacy [is] not a word we'd use really (Project Manager)*	1

Table 2: Threat & Risk Analysis, and Customer Need for Security

	Threat & Risk Analysis				Security for Customers		
	Formal	Informal	Neither		Required	(Both)	Valued
NHS	6	1			3	3	1
B2B	4	1	2		0	3	4
Consumer	3	1	2		2	4	0

> *interview all your programmers and to check your private key on that device... So, if you just like to disclose what your private key is on that. No. How do I know it's a good one? ... So, the result was they started putting cameras into cash machines. Because now I can show a picture of you withdrawing the money (Chief Strategy Officer)*

Of the three participants who did not use stories in their interviews, one stated that their team used stories 'frequently', and two that their teams used them 'sometimes'. So, all were familiar with the use of such stories.

Approach to Security and Privacy Decision Making

In exploring our predictions PR3 (*not analyze threats and risks*) and PR4 (*security and privacy not saleable*), we expected both to be heavily influenced by customer requirements. We accordingly analyzed the results by customer type: 'NHS' for the National Health Service, the primary UK healthcare provider; 'B2B' for products and services sold to other businesses; and 'Consumer' for products sold directly to end users.

To our surprise, many participants used **threat and risk analysis**, in some cases to a very impressive level. Table 2 (left) highlights the number of participants who used formal threat assessment with documented outcomes; who used informal threat assessment; or who mentioned neither.

For **security sales**, we observed that in many ways the security of a product might be *required* to make a sale but not *valued* by customers as a 'selling point'. Instead, customers would expect the security to be present. Table 2 (right) shows how participants described their own product sales.

Thematic Analysis

The open coding generated an initial 34 codes. Table 3 shows the 27 codes from which themes were identified, excluding topics outside the scope of the research questions. Colored cells show participants' contributions to each. Codes are sorted top to bottom in decreasing order of number of the number of contributing participants; participants are in order of interview date, leftmost first.

The right-hand side of Table 3 shows that the coding of the last 7 participants generated no new codes. This 'thematic saturation' suggests that the sample of 20 interviews was probably sufficient to capture all relevant themes.

The categorization process grouped these codes into six themes: the dominance of compliance, health as a complex hybrid domain, mechanisms for prioritization, the decision maker ecosystem, the complexity of the decisions to make, and the factors influencing decisions. Table 3's column 'T' shows the theme number associated with each code.

The following sections describe each of the themes, including quotations from interviewees. Codes from Table 3 are in *italics*.

Theme 1: Dominance of Compliance

A much-repeated topic was standards *compliance,* which affected most of the participants:

> *I assess what our requirements are to legally release the product in compliance with […] the medical device regulations (Product Manager)*
>
> *[It's] making sure you conform to some normal industry standards like ISO27001, GDPR. Cyber Essentials is another one we get asked for (Chief Technical Officer)*

Some standards require a *responsible individual for security* issues. But the standards cited, excepting GDPR and Cyber Essentials, relate largely to safety and confidentiality rather than cybersecurity.

> *There's not really a [standard] … for the security of our IT systems (Consultant)*

However, many safety-related standards mandate a rigorous, fully documented, risk-based approach. Participants found that well-suited to addressing cybersecurity-related issues:

> *And in the process of ensuring that for safety that also works for security as a sort of side benefit. (Consultant)*

Given the importance of privacy to compliance, some saw cybersecurity simply as *security to ensure privacy*; one also needed *security to support reliability.*

Theme 2: Complex Hybrid Domain

Most participants mentioned the complexity of the domain. Projects may have many *different stakeholders for security*, such as medical staff, investors, and purchasing teams. They also reported a range of *varied requirements* for cybersecurity:

> *Like in the USA is the HIPPA, and in Europe it will be the GDPR (Chief Technical Officer)*

It also became clear as the interviews progressed that 'Health IoT' was not one but *several different domains*. For example, the requirements for home monitoring were very different from implanted devices.

Table 3: Codes Discussed by Each Participant, with Relevant Theme Numbers

Code	T	Participants discussing code
Auditing	5	
Compliance	1	
Decisions and prioritisation	3	
Different domains	2	
Different stakeholders for security	2	
Limited concern over threats	6	
Long software lifetimes	5	
Need for secure software updating	5	
Need to reassure stakeholders	4	
Operations required around security and privacy	5	
Product manager committee	4	
Responding to events	5	
Responsible individual for security	1	
Security and priv. implications on wider environment	6	
Security and privacy a battle with clients	4	
Security and privacy are expensive	6	
Security and privacy as a means to avoid litigation	6	
Security and privacy considered good housekeeping	6	
Security to enforce privacy	1	
Security to support reliability	1	
Small companies	6	
Smuggling in security	4	
Start-ups limited security	6	
Trust	6	
Users private from developers	5	
Varied requirements	2	
Ways to avoid security and privacy needs	6	

Theme 3: Range of Mechanisms for Prioritization

A frequent theme that emerged from the analysis was, unsurprisingly, *decisions and prioritization*: approaches for decisions about the prioritization of security and privacy activity against other development. Seven of the participants described a score-based risk assessment approach. Using a score basis makes the decision one that the technical team could take without (necessarily) needing product manager input:

> *We rate its importance; we rate how much work it will be to address it. And then we divide those two… It gives you a way of prioritizing which issues you should be working out (Managing Director)*

Of the other participants, eight described a less process-driven approach, where the decisions were solely made by product management. Others did not identify a specific mechanism.

Theme 4: Decision Maker Ecosystem

Agile methodologies often expect decisions to be made by a single 'Product Owner' [9]. However, the decision-making processes described involved a much wider range of stakeholders. Five of the participants described decision making by a *product management committee*, of senior and expert staff. Other concerns were a *need to reassure stakeholders*; and sometimes that *security and privacy [was] a battle with clients:*

> *It is an upwards battle to try and get clients to be fully aware of the implications of cyber, not just from a security point of view, but from the return-on-investment point of view. (CEO)*

Indeed, some mentioned sidestepping this battle by *smuggling in security*, without stakeholder knowledge.

Theme 5: Complexity of Decisions

There were some noteworthy complexities to the threat assessment process. Participants stated that many of the medical devices have *long software lifetimes*, and even more have a need for *secure software updating*. Evaluating problems in the field also presented issues, particularly keeping *users private from developers*.

Further, though the survey was about software development, the threat assessment implications for most of the organizations were far wider in scope. Many participants

Table 4: Further Factors to Security and Privacy Decisions

Factor	Example
Limited concern over threats	*I don't think for the most part people are trying to hack [medical] devices. (Chief Strategy Officer)*
Trust	*The main issue here is trust… If you lose that security, you will lose [your customers'] trust. (Chief Executive Officer)*
Security and privacy a means to avoid litigation	*At the end of the day, because of the potential litigation, you know, privacy is a key thing. (Developer)*
Security and privacy considered as default or good housekeeping	*I think privacy stuff is built in right from the start, so it's taken as a given. There's best practice to follow for that. (Developer)*
Security and privacy are expensive	*There's a very high cost: security and privacy … etc. It is expensive to do properly, but it is even more expensive in the context of the NHS. (Founder and Product Manager)*
Ways to avoid security and privacy needs	*If we needed Bluetooth in a safety critical product, we might split it and have two controllers, with one that does the safety critical thing. Then you have to … have appropriate barriers between the two. (Consultant)*
Security and privacy implications related to wider environment	*Getting a connection to [a secure NHS network] was a huge thing, but … to have [that] does require a lot of reassurances that you meet various criteria (Developer).*
Small companies and Start-ups	*The security side is a worry, but we're not big enough that we have a big target on our back (Product Manager)*

mentioned the *operations required around security and privacy*, and particularly *responding to events*. A further important issue was *auditing*, supporting third-party assessments of the organization's security compliance.

Theme 6: Variety of Factors Influencing Decisions

Finally, a major theme of the discussions was about the factors influencing security and privacy decisions. Table 4 illustrates eight examples.

Limitations

As with any survey, there are limitations in how far we can take the conclusions. Specifically, we can identify two concerns in our analysis of the survey:

Generalizability: The thematic saturation suggests that the findings are generalizable to any software development teams in small and medium Health and Health IoT companies in the UK. Though a few interviewees were from further afield, we have no basis for deductions about similar companies outside the UK or in other fields.

Potential for bias: the randomness of the recruitment approach means this is likely to be a representative sample of small and medium organizations in the Health IoT domain. There is, though, a possibility of systemic bias in the recruitment.

Conclusions

Returning to this article's goal, to enable security specialists and academics to support isolated HIoT development teams as effectively as possible, we can draw out three conclusions, as follows.

Conclusion 1: Take care with language when working with developers. From the survey's exploration of prediction PR1 (*inconsistency in understanding of key concepts with that of security experts*), we found the prediction was largely correct. Figure 2 showed that the use of key security and privacy terms appears superficially similar to that of cybersecurity experts. However, Figure 3 showed that the meanings attached to those terms are often different. So, while many use 'event' or 'incident' with the cybersecurity-standard meaning, very few used 'threat' with its corresponding meaning. Also, few used 'threat actor' or 'victim'—or even had terms for those concepts. Almost all used more specific terminology for their context instead of these two terms. Yet participants' understanding and definitions for 'security' and, to a lesser extent, 'privacy' were generally accurate and tailored to their own project contexts.

From this, we conclude that, while cyber experts will probably understand the terms used by developers, we cannot assume that developers will understand cyber experts. Specifically, when working with HIoT developers, there is little need for cyber experts to explain the concepts of 'security' and 'privacy'. And 'event' is likely to be understood., 'A risk', though, might be a better term to use than 'a threat'. And if the concepts of 'threat actor' or 'victim' are needed they will require definition and explanation.

Conclusion 2: Use stories to communicate. The prediction PR2, (*developers use stories*) also proved correct, with 18 of the 20 interviewees describing story use in their projects and 17 using stories themselves. This suggests both that stories

are a good way to communicate concepts and knowledge; and that stories are likely to be well-received by isolated HIoT developers. We can conclude that stories are a useful tool to communicate with most, if not all, HIoT development teams.

Conclusion 3: Empower teams to support the complex decision-making process. We found that prediction PR3 (*not analyze threats and risks*) was not supported by the survey. All the participant companies supplying the NHS, and a clear majority of the remainder, carried out threat assessments. In most cases this was a formal written process. Fifteen of the 20 also had a clear process to prioritize the mitigation of identified problems. Seven, indeed, described a numerically driven process, potentially allowing prioritization independently of product management. We can conclude that, in the HIoT domain at least, there may be little need to teach risk-based threat assessment from scratch.

Prediction PR4 (*security and privacy not saleable*) also proved incorrect. There were no participants for whom security and privacy were not either required or valued, in one way or another, by customers. The 'entry stakes' requirements were generally compliance standards related to the product. They impacted more than just the software: auditing, cybersecurity operations, and defect tracking were concerns for many participants. We conclude that in HIoT it may be inappropriate to promote cybersecurity and privacy as a novel sales approach.

It was clear in the thematic analysis that compliance related to safety and privacy was an essential driver in most HIoT cybersecurity and privacy. Therefore, any support could productively be motivated via these compliance requirements.

However, a major challenge for support is clearly the complexity of the decision landscape. The range of considerations in Table 4 alone shows that attempting to simplify decisions would be both inappropriate and unhelpful.

Assuming a single decision-maker to influence would also be incorrect; security and privacy decisions were often made by committees.

We conclude that couching support to isolated HIoT development teams as direct instructions or externally imposed 'secure development lifecycles' [11] is likely to fail. Instead, such support might contribute to existing decision-making processes by empowering the teams to work with stakeholders to make better decisions. Possibilities for such support might be providing industry risk information or approaches to improve threat analysis.

Summary

This paper describes a survey of 20 experts working in small to medium enterprises in the Health, and predominantly the Health Internet of Things, domain. The results suggest that any intervention working with HIoT developers can profitably:

- Assume a working understanding of the terms 'security' and (usually) 'privacy';
- Expect, but not rely on, a knowledge of risk-based threat assessment;
- Assume a need for security or privacy from their customers (but not that either may necessarily be a sales point);
- Motivate security in terms of compliance with existing safety and privacy standards;
- Avoid, or take great care with, terms such as 'threat', 'risk', 'threat actor' and 'victim';
- Use stories to express cyber 'threats' in an easily understandable way; and
- Avoid approaches that over-simplify the complexity of decision-making, such as providing direct 'how to' instructions.

We observe also that the survey instrument and method can support similar research addressing any other domain.

This guidance offers clear direction to anyone creating an intervention to use with HIoT developers, especially those isolated from security professionals. It also suggests possibilities and a well-defined approach to consider for development teams in any other domain.

Using this guidance will help security specialists and academics to support Health Internet of Things, and other, development teams. That will lead to vital improvements in the security of the software systems on which we all rely.

Acknowledgement and Access

This research was funded through the UK PETRAS National Centre of Excellence for IoT Systems Cybersecurity under EPSRC grant number EP/S035362/1.

References

[1] Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M.L., and Stransky, C. How Internet Resources Might Be Helping You Develop Faster but Less Securely. *IEEE Security and Privacy 15*, 2 (2017), 50–60.

[2] Ando, H., Cousins, R., and Young, C. Achieving Saturation in Thematic Analysis: Development and Refinement of a Codebook. *Comprehensive Psychology 3*, (2014).

[3] Bell, L., Brunton-Spall, M., Smith, R., and Bird, J. *Agile Application Security: Enabling Security in a Continuous Delivery Pipeline*. O'Reilly, Sebastopol, CA, 2017.

[4] Braun, V. and Clarke, V. Thematic Analysis. In H. Cooper, ed., *APA Handbook of Research Methods in Psychology, Vol 2: Research Designs*. American Psychological Association, 2012, 57–71.

[5] Campbell, J.L., Quincy, C., Osserman, J., and Pedersen, O.K. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods and Research 42*, 3 (2013), 294–320.

[6] Konecki, K.T. Visual Grounded Theory: A Methodological Outline and Examples from Empirical Work. *Revija za Sociologiju 41*, 2 (2011), 131–160.

[7] National Initiative for Cybersecurity Careers and Studies. Cybersecurity Glossary. 2022. https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[8] Sun, Y., Lo, F.P.W., and Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access 7*, (2019), 183339–183355.

[9] Sutherland, J. and Schwaber, K. The Scrum Guide. https://scrumguides.org/index.html.

[10] Weir, C., Becker, I., and Blair, L. A Passion for Security: Intervening to Help Software Developers. *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, IEEE (2021), 21–30.

[11] de Win, B., Scandariato, R., Buyens, K., Grégoire, J., and Joosen, W. On the Secure Software Development Process: CLASP, SDL and Touchpoints Compared. *Information and Software Technology 51*, 7 (2009), 1152–1171.

[12] Zaldivar, D., Tawalbeh, L.A., and Muheidat, F. Investigating the Security Threats on Networked Medical Devices. *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, Institute of Electrical and Electronics Engineers Inc. (2020), 488–493.

Charles Weir is a Research Fellow at Lancaster University. With a background running software development projects, he now researches helping development teams improve software security.

Anna Dyson researches international relations at Lancaster University, specializing in the use of interdisciplinary perspectives and creative approaches. She studies the convergence of artificial intelligence, unmanned systems and the cyber domain.

Dan Prince Is a Senior Lecturer in cybersecurity at Lancaster University. His work focuses on cyber threat intelligence and risk management, and specifically the exploration of quantitative methods in these fields.