Using Card Sorting to Classify Elements of the Security Risk Management Program for Medical Devices

Nadica Hrgarek Lechner
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
nhrgarek@foi.hr

Abstract. *Establishing a security risk management program for medical devices can be challenging. Medical device manufacturers must understand which elements of the program are required, optional, or unnecessary to make effective decisions. By prioritizing the most important elements, manufacturers can establish a robust security risk management program.*
This paper identifies 40 elements of the security risk management program for medical devices. Using closed card sorting, professionals within the medical device sector classified these elements into predefined categories. The study involved 53 participants who completed two card sorts using an online tool over a period of five weeks.

Keywords. card sorting, card sort, closed cart sorting, cybersecurity, medical devices, security risk management

1 Introduction

In recent years, regulators have been increasing their focus on cybersecurity of medical devices. Medical device cybersecurity regulations, standards, and guidelines keep rising worldwide. To cope with the new situation, medical device companies are adjusting the processes and structures they need to ensure compliance with relevant regulations.

Medical device manufacturers need to perform security risk management for medical devices that are subject to cybersecurity during their total product life cycle. This applies to new product development as well as to legacy medical devices that cannot be reasonably protected against current cybersecurity threats. Due to increasing regulatory requirements, establishing and maintaining a comprehensive security risk management program for medical devices can be a daunting task. An effective program needs to be integrated into the manufacturer's quality (management) system, as well as be robust and flexible to respond to changes.

This paper provides 40 elements to be considered when establishing and maintaining the security risk management program for medical devices. The elements have been categorized by study participants into predefined categories using closed card sorting. *Card sorts* are the simplest form of sorts, in that the entities being sorted are simply names on cards (Rugg & McGeorge, 1997, p. 84). There are two primary types of card sorts: open and closed. Open card sort allows the participants to create their own categories. In a closed card sort, participants have to sort a list of items into a predefined set of category names provided by a researcher. Participants are constrained and cannot update category names or add new categories.

The paper is organized as follows. Section 2 provides an overview of the security risk management program for medical devices. The research approach is described in section 3. Section 4 presents and discusses the key results of the study. The final section of the paper restates the research problem, summarizes the main findings from the study, discusses the implications of the research findings and the limitations related to the research problem, and proposes new directions for future research.

2 Security Risk Management Program for Medical Devices

Effective cybersecurity management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity (FDA, 2014, p. 2). Ray (2021, p. 19) states that an alternative risk modeling approach for medical device cybersecurity is needed, with a threat modeling approach driving the identification of risk factors.

According to FDA guidances (2014, 2016), security risk management is applicable to:

- Medical devices that contain software (including firmware) or programmable logic,

- Software that is a medical device (including mobile medical applications),
- Medical devices that are considered part of an interoperable system, and
- Legacy devices.

Security risk management for medical devices is an ongoing process and not a one-time activity. The security risk management process shall include the following elements: security risk analysis, security risk evaluation, security risk control, evaluation of overall security residual risk acceptability, security risk management review, and production and post-production activities (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023, pp. 10–11). According to (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023, p. 12), production and post-production activities include: vulnerability monitoring process associated with manufacturer-developed software and third-party components, establishing a threat intelligence program or using membership to ISAOs or similar organizations of threat intelligence sources, security incident response plan, vulnerability disclosure and communication plans, establishment of a customer communication process, periodic reviews of security risk controls and the security landscape, and identification of vulnerabilities and development, testing, and deployment of security patches.

Having the security risk management program in place is necessary to take a systematic approach to managing security risks throughout the total medical device life cycle and to achieve regulatory compliance. The program helps to determine which security risks have the highest impact, and to mitigate risks and minimize damage, when a medical device security incident occurs. Once implemented, the security risk management program needs to be continuously updated and improved to keep up with regulatory changes in the medical device industry.

3 Research Approach

Card sorting is one of techniques that can be used for knowledge elicitation (Barrett & Edwards, 1995). According to Fincher & Tenenberg (2005, p. 89), card sorting is a categorization task. Spencer (2009, p. 69) recommends using 30–100 cards for card sorting. U.S. Department of Health and Human Services (2013) recommends 30 to 40 cards at the absolute outside, especially for an open sort. Tullis and Wood (2004) conducted a study to assess the minimum number of participants for a card-sorting study. They found that reasonable structures are obtained from 20–30 participants. Lantz et al. (2019, p. 654) found that the most efficient number of participants for method of card sorting or pairwise comparisons was approximately 10–15. Nielsen (2004) recommends to test 15 users for card sorting to reach a correlation of 0.90, 20 users to reach 0.93, and 30 users to reach 0.95.

Up to the author's best knowledge, this study is the first attempt to use card sorting to classify elements of the security risk management program for medical devices. The study was guided by the following research questions:

1. How can a security risk management program for medical devices be characterized?
2. How professionals within the medical devices sector from various backgrounds and roles would classify elements of the security risk management program for medical devices into logical categories?
3. What is the order of perceived needs for elements of the security risk management program for medical devices?
4. What are the respondents' views on the elements of the security risk management program for medical devices?

To answer the first research question, a narrative literature review was conducted to identify elements of the security risk management program for medical devices. After reviewing cybersecurity standards, technical information reports, and guidances for medical devices and taking into consideration the results of a scoping study (Hrgarek Lechner, 2021), recommendations for creating a Product Cybersecurity Organization (Ray, 2021, pp. 22–23) and defining roles and responsibilities (Wirth et al., 2020), author's experience with the security risk management, and the recommended number of cards for card sorting, 40 elements of the security risk management program for medical devices were derived (refer to Table 1). Preparing the list of elements to produce a set of cards with brief descriptions was the most challenging and time-consuming activity.

The second, third, and fourth research questions were answered by conducting an online survey and analysing and interpreting collected quantitative data and qualitative data including participant comments. The survey was developed with Qualtrics Surveys tool. The survey was reviewed by one subject matter expert who is familiar with the security risk management process of medical devices. Two experts from academia were consulted to get feedback about the content and questionnaire design. After received feedback was addressed, the survey link was sent to potential survey participants. The survey contained two unmoderated card sorting activities where participants were asked to sort the same set of cards using a different criterion for the sorting each time. The order of cards was randomized to guard against sorting bias. Each card was presented using the carousel view in Qualtrics Surveys. After choosing a category for a card, a participant automatically progressed to the next card. The participants were allowed to skip cards.

Collecting responses from survey participants took five weeks and no personally identifiable information

and other identifiers (i.e., IP address, location data) were collected. Data was collected from a convenience sample of cybersecurity professionals with domain knowledge within the medical devices sector (i.e., practitioners, consultants, auditors, and academic researchers who are involved in security risk management tasks of medical devices and have at least one year of relevant experience in this area).

LinkedIn professional network was primarily used to identify and recruit qualified participants for the study. The survey link was sent individually to 328 potential participants via LinkedIn and to 4 potential participants via e-mail. It was anticipated that up to 20 survey respondents will be recruited. Survey scams and phishing links are common concerns when using online surveys, especially when cybersecurity professionals participate in online surveys. Few contacted people expressed security concerns about clicking on the provided survey link and refused to participate. One participant asked a question that only the survey author could answer to get confidence that the author's LinkedIn account was not hacked and the survey link is safe.

The total number of individuals who attempted the card sort was 57. The results presented in this paper are from 53 survey participants who truly attempted the sort. Section 4 summarizes and discusses the results of the card sorting exercises.

Table 1. Elements of the security risk management program for medical devices

Nr.	Element	Source
1	**Compliance with applicable cybersecurity laws, regulations, standards, and guidances** for medical devices	Author's own work
2	**Monitoring of regulatory changes and developments** in cybersecurity laws, regulations, standards, and guidances for medical devices	Author's own work
3	**A dedicated team of product security professionals**	Derived from (Ray, 2021)
4	**Qualified and trained personnel** performing security risk management tasks	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
5	**Organizational roles and responsibilities** for security risk management	Derived from (*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023), and (Wirth et al., 2020)
6	**Secure product development life cycle/framework**	(*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), (FDA, 2022)
7	**Secure product development training for employees**	Author's own work
8	**Glossary of terms and definitions** relating to medical device cybersecurity	Author's own work
9	**Security risk management process** that is coordinated with other medical device risk management processes	(*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
10	**Integrated security risk management process into a quality (management) system**	(*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), (FDA, 2022)
11	**Integrated security risk management process with accompanying processes** such as vulnerability handling, vulnerability disclosure, incident response, etc.	(FDA, 2016), (FDA, 2022)
12	**Internal/quality audits** of the security risk management program	Derived from (FDA, 2022)
13	**Measures and metrics** for processes that reduce the number and severity of vulnerabilities in products	(FDA, 2022)
14	**Software tools** to support security risk management tasks	Derived from (FDA, 2016)
15	**Security risk assessment** of a product	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016)
16	**Security risk assessment of third-party software/firmware components** incorporated within a product	(FDA, 2022)
17	**Security assessment of unresolved software anomalies** that exist in a product at the time of regulatory submission	(FDA, 2022)
18	**Threat modeling process**	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2016),

Nr.	Element	Source
		(*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019), (Medical Device Coordination Group, 2020), (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), (FDA, 2022), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
19	Determined **security risk controls** to reduce security risks	(FDA, 2014), (*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2022), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
20	Implemented and tested **security risk controls**	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2022)
21	**Security architecture** providing the security context and trust boundaries of a medical device system	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2022)
22	**Security requirements** for the product under development	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2022)
23	**Labeling** to communicate relevant security information to users of medical devices	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (FDA, 2022)
24	**Software Bill of Materials (SBOM)**	(*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019), (Medical Device Coordination Group, 2020), (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), (FDA, 2022), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023), (FDA, 2023)
25	**Premarket security testing** to identify and address potential vulnerabilities prior to exploitation	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (Medical Device Coordination Group, 2020), (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), (FDA, 2022)
26	**Security risk management artifacts** (e.g., security risk management plan, security risk analysis, security risk management report, etc.)	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
27	**Security risk management documentation** for regulatory submissions	(FDA, 2014), (FDA, 2022)
28	**Security training for users** of medical devices	Derived from (FDA, 2016) and (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
29	**Post-market periodic security testing**, including penetration testing	Derived from (FDA, 2022)
30	**Monitoring of third-party software/firmware components** incorporated within a product to identify and detect potential vulnerabilities	(FDA, 2016), (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019)
31	**Monitoring of cybersecurity information sources** to identify and detect potential security threats and vulnerabilities that may affect medical devices	(FDA, 2016), (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019)
32	Medical device manufacturers participation in a health focused **Information Sharing Analysis Organization (ISAO)**	(FDA, 2016), (*AAMI TIR57: Principles for medical device security–Risk management*, 2016), (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023)
33	**Vulnerability management process**	Derived from (FDA, 2016) and (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019)
34	**Vulnerability management plans**	(FDA, 2022)
35	**Security risk assessment of post-market vulnerabilities**	(FDA, 2016)
36	**Patch management process** for providing post-market security patches and updates	(*AAMI TIR57: Principles for medical device security–Risk management*, 2016),

Nr.	Element	Source
		(*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019), (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021)
37	**Product security incident response process**	Derived from (FDA, 2016) and (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019)
38	**Coordinated vulnerability disclosure process**	(FDA, 2016), (*AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers*, 2019), (*ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers*, 2023), (FDA, 2023)
39	**Post-market surveillance system** including cybersecurity considerations	(Medical Device Coordination Group, 2020)
40	**Vigilance process** for reporting serious incidents and field safety corrective actions related to cybersecurity incidents	(Medical Device Coordination Group, 2020)

4 Results and Discussion

As shown in Fig. 1, a total of 68 Qualtrics Survey responses were recorded during the data collection period from May 8th, 2023 to June 11th, 2023.

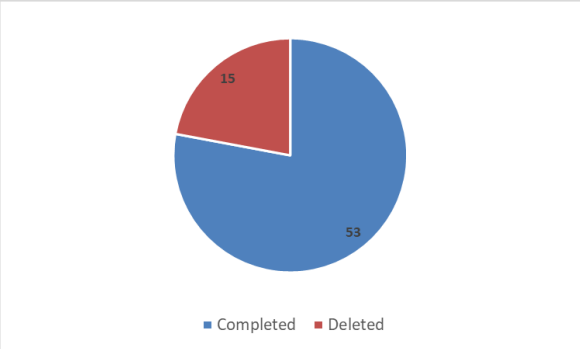

Figure 1. Recorded responses by status

Prior to data analysis, all recorded responses in Qualtrics Survey were screened. Survey data cleaning was performed to identify and remove preview responses as well as incomplete and suspicious responses from participants who don't match target audience criteria, did not complete the card sorting exercises, had only a small number of cards 'sorted' leading to incomplete sorts, or offered nonsensical feedback in open-ended questions.

15 recorded responses were deleted from dataset (Fig. 1) in the following cases:

- 2 preview responses were used only for testing the survey and not to record real data.
- 1 participant did not give consent and no data was collected.
- 2 participants gave consent, but did not answer any survey question.
- 1 participant had less than 1 year of experience and participated only in 1 medical device project that involved cybersecurity. In addition, the participant placed 23 out of 40 cards consecutively in one category in the first card sorting exercise and only sorted one card in the second card sorting exercise.
- 6 participants answered the demographic and context questions, but did not complete any card sorting exercise.
- 3 participants only partially completed card sorting exercises leading to incomplete sorts.

Participants who do not have adequate familiarity with the items being sorted may reduce the effectiveness of card sorting. Two participants had less than 1 year of experience in security risk management activities of medical devices and did not meet target audience criteria. However, they were familiar with the security risk management process of medical devices and participated in 2-5 medical device projects that involved cybersecurity. For these reasons, their responses were not deleted from dataset.

Demographic characteristics of survey participants are illustrated in Fig. 2 – Fig. 6. Fig. 7 and Fig. 8 present context data.

As shown in Fig. 2, the large majority of the respondents (69.8%) represented companies with more than 1000 employees.

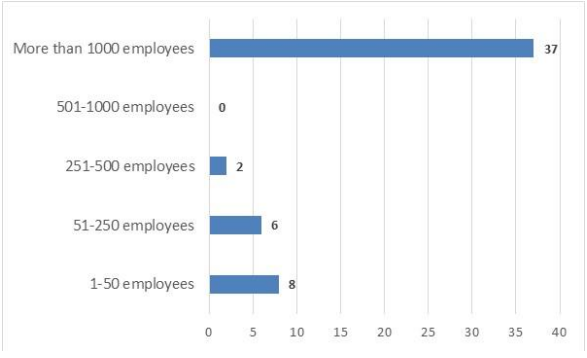

Figure 2. Responses per company size

Fig. 3 represents the geographic location of company's headquarters.

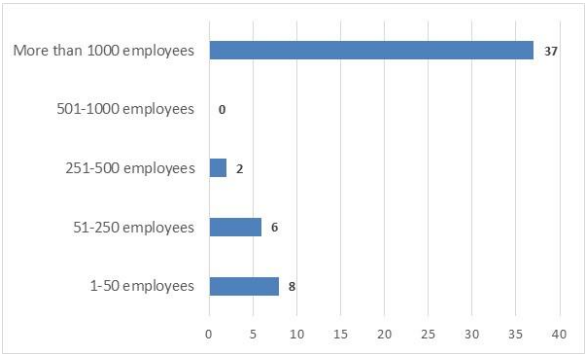

Figure 3. Responses per company headquarters location

Security risk management of medical devices involves participation of stakeholders from various areas. Participants were asked to select one or more applicable job roles and their answers are displayed in Fig. 4. Four respondents specified other job roles as follows: Quality Management, Head of Development, Regulatory Consultant, Director of Product Security.

Figure 4. Responses per current job role within the organization

As shown in Fig. 5, the majority of respondents were very familiar (45.2%) and extremely familiar (39.6%) with the security risk management process for medical devices.

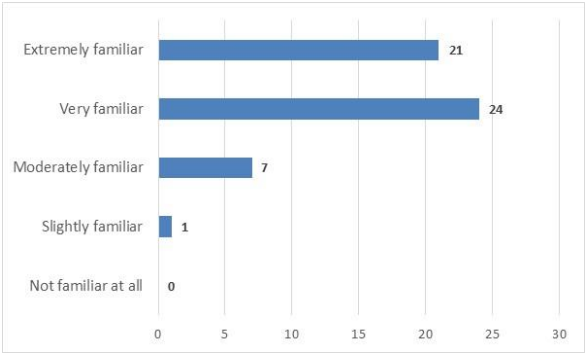

Figure 5. Responses per familiarity with the security risk management process for medical devices

As depicted in Fig. 6, 39.6% of respondents had more than 6 years of experience in security risk management activities of medical devices.

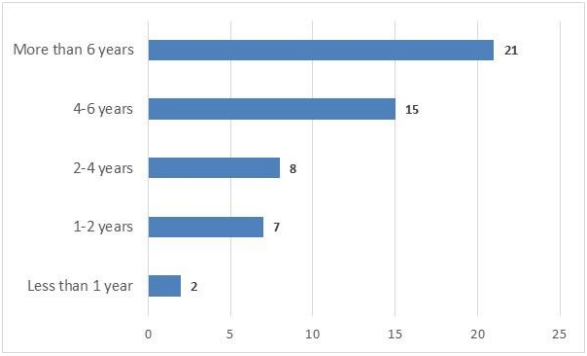

Figure 6. Responses per years of experience in security risk management activities of medical devices

As illustrated in Fig. 7, 50.9% of respondents participated in more than 10 projects involving cybersecurity.

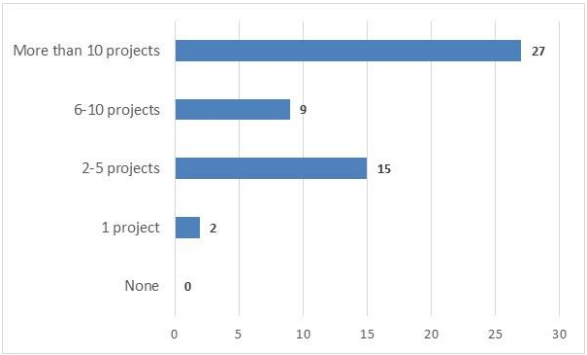

Figure 7. Responses per number of medical device projects involving cybersecurity

According to Fig. 8, the majority of respondents used hybrid approach (59.6%) to assess security risk in medical device projects. Quantitative approach was used by only 13.5% of respondents. 1 of 53 participants did not provide answer.

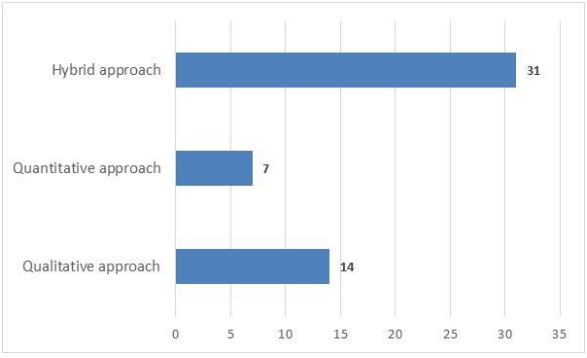

Figure 8. Responses per approach to assess security risk in medical device projects

Survey participants were asked to categorize a set of 40 items (i.e., cards) representing elements of the security risk management program for medical devices into predefined categories using a different criterion for the sorting each time. The goal was to understand how the participants would group these items into categories. In total, 52 responses were collected for the first card sorting exercise with five predefined categories and 51 responses were collected for the second card sorting exercise with three predefined categories.

In the first card sort, survey participants were asked to categorize a set of 40 cards into five predefined categories: "Regulatory compliance", "Product security governance", "Security risk management", "Total product life cycle", *"Uncategorized"*. Participants were instructed to use a special category *"Uncategorized"* for cards that don't fit with anything. Table 2 summarizes what percentage of respondents placed each card into each predefined category and shows the most popular clusters of cards for each category based on where respondents placed the cards most often. The cards in the matrix were reordered according to which cards have the highest percentages among all of the categories and the cards with the same popular category are clustered together. Within the clusters, the cards are sorted in descending order by the percentage of respondents who placed them in that category. The percentage of each grouping within the cluster is also visually represented by different shades of grey colour as follows: ☐ 0%, ☐ 1–25%, ☐ 26–50%, ☐ 51–75%, ☐ 76–100%. The darker the shade, the more the percentage. In two cases, a card was placed into two different categories at equal percentages (refer to table cells marked with a dashed rectangle). Individual responses were screened and the cards were clustered to the category that received responses from a higher number of respondents who rated their familiarity with the security risk management process for medical devices as extremely familiar.

Table 2 provides an overview about all categories that a card was placed. It shows four clusters with higher agreement rates for the specific cards most respondents agree to belong to those predefined categories. "Regulatory compliance" and "Security risk management" are the most popular categories. Out of total 40 cards, the respondents placed 15 cards (37.5%) into the special category *"Uncategorized"*. Most cards were placed in a number of categories. This may indicate that categories overlap or card labels are not clearly defined. Feedback was received from two participants who attempted the first card sort that some of the categories are overlapping.

Table 2. Agreement matrix of the first card sorting exercise

Card #	Card name	Category				
		Regulatory compliance	**Product security governance**	**Security risk management**	**Total product life cycle**	***Uncategorized***
27	**Compliance with applicable cybersecurity laws, regulations, standards, and guidances** for medical devices	86.5%	9.6%	0%	3.8%	0%
10	**Monitoring of regulatory changes and developments** in cybersecurity laws, regulations, standards, and guidances for medical devices	78.8%	7.7%	3.8%	7.7%	1.9%
30	**Security risk management documentation** for regulatory submissions	67.3%	5.8%	19.2%	7.7%	0%
14	**Labeling** to communicate relevant security information to users of medical devices	48.1%	11.5%	19.2%	17.3%	3.8%
6	**Vigilance process** for reporting serious incidents and field safety corrective actions related to cybersecurity incidents	46.2%	19.2%	11.5%	23.1%	0%
38	**Internal/quality audits** of the security risk management program	40.4%	26.9%	13.5%	11.5%	7.7%
31	**Organizational roles and responsibilities** for security risk management	11.5%	53.8%	28.8%	1.9%	3.8%
34	**Measures and metrics** for processes that reduce the number and severity of vulnerabilities in products	1.9%	51.9%	26.9%	15.4%	3.8%
2	**A dedicated team of product security professionals**	1.9%	50%	26.9%	21.2%	0%
7	**Secure product development training for employees**	17.3%	44.2%	7.7%	23.1%	7.7%
39	**Coordinated vulnerability disclosure process**	17.3%	38.5%	21.2%	19.2%	3.8%
40	**Vulnerability management plans**	3.8%	36.5%	30.8%	26.9%	1.9%
28	**Glossary of terms and definitions** relating to medical device cybersecurity	13.5%	34.6%	9.6%	9.6%	32.7%

Card #	Card name	Category				
		Regulatory compliance	**Product security governance**	**Security risk management**	**Total product life cycle**	***Uncategorized***
12	Medical device manufacturers participation in a health focused **Information Sharing Analysis Organization (ISAO)**	19.2%	30.8%	19.2%	15.4%	15.4%
13	**Product security incident response process**	23.1%	25%	25%	23.1%	3.8%
17	Determined **security risk controls** to reduce security risks	1.9%	5.8%	84.6%	7.7%	0%
21	**Security risk assessment** of a product	3.8%	11.5%	78.8%	5.8%	0%
24	**Security risk management artifacts** (e.g., security risk management plan, security risk analysis, security risk management report, etc.)	13.5%	7.7%	75.0%	3.8%	0%
5	**Threat modeling process**	3.8%	11.5%	71.2%	11.5%	1.9%
22	Implemented and tested **security risk controls**	0%	7.7%	63.5%	25%	3.8%
37	**Security risk assessment of third-party software/firmware components** incorporated within a product	3.8%	17.3%	61.5%	17.3%	0%
19	**Security risk assessment of post-market vulnerabilities**	9.6%	9.6%	59.6%	21.2%	0%
3	**Security risk management process** that is coordinated with other medical device risk management processes	11.5%	3.8%	55.8%	25%	3.8%
23	**Security assessment of unresolved software anomalies** that exist in a product at the time of regulatory submission	11.5%	9.6%	53.8%	21.2%	3.8%
20	**Software tools** to support security risk management tasks	0%	17.3%	51.9%	19.2%	11.5%
33	**Integrated security risk management process with accompanying processes** such as vulnerability handling, vulnerability disclosure, incident response, etc.	3.8%	32.7%	42.3%	19.2%	1.9%
15	**Monitoring of cybersecurity information sources** to identify and detect potential security threats and vulnerabilities that may affect medical devices	1.9%	30.8%	42.3%	25%	0%
36	**Vulnerability management process**	3.8%	25%	40.4%	28.8%	1.9%
18	**Qualified and trained personnel** performing security risk management tasks	11.5%	36.5%	38.5%	9.6%	3.8%
26	**Premarket security testing** to identify and address potential vulnerabilities prior to exploitation	7.7%	25%	38.5%	28.8%	0%
9	**Security architecture** providing the security context and trust boundaries of a medical device system	1.9%	30.8%	34.6%	32.7%	0%
1	**Secure product development life cycle/framework**	1.9%	13.5%	7.7%	76.9%	0%
35	**Patch management process** for providing post-market security patches and updates	1.9%	13.5%	19.2%	65.4%	0%
25	**Monitoring of third-party software/firmware components** incorporated within a product to identify and detect potential vulnerabilities	7.7%	19.2%	26.9%	44.2%	1.9%
4	**Security requirements** for the product under development	13.7%	15.7%	25.5%	43.1%	1.9%
32	**Post-market periodic security testing**, including penetration testing	11.5%	17.3%	30.8%	38.5%	1.9%
11	**Post-market surveillance system** including cybersecurity considerations	36.5%	11.5%	15.4%	36.5%	0%
8	**Software Bill of Materials (SBOM)**	25%	19.2%	19.2%	32.7%	3.8%
16	**Security training for users** of medical devices	21.2%	21.2%	13.5%	26.9%	17,3%
29	**Integrated security risk management process into a quality (management) system**	19.2%	21.2%	25%	26.9%	7.7%

In the second card sort, survey participants were asked to categorize the same set of 40 cards into three predefined categories: “Required”, “Optional”, “Not necessary”. Table 3 shows the agreement matrix. A

value of 100% means that all respondents placed the card in the category. The agreement matrix shows two clusters with higher agreement rates for the specific cards most respondents agree to belong to those predefined categories. Out of total 40 cards, the respondents placed 4 cards (10%) into the category "Optional". It was expected that the card "**Security training for users** of medical devices" will be categorized as "Required". However, 55% of the respondents categorized this card as "Optional".

Table 3. Agreement matrix of the second card sorting exercise

Card #	Card name	Category		
		Required	**Optional**	**Not necessary**
1	**Secure product development life cycle/framework**	100%	0%	0%
17	Determined **security risk controls** to reduce security risks	100%	0%	0%
21	**Security risk assessment** of a product	100%	0%	0%
22	Implemented and tested **security risk controls**	100%	0%	0%
25	**Monitoring of third-party software/firmware components** incorporated within a product to identify and detect potential vulnerabilities	100%	0%	0%
27	**Compliance with applicable cybersecurity laws, regulations, standards, and guidances** for medical devices	100%	0%	0%
3	**Security risk management process** that is coordinated with other medical device risk management processes	100%	0%	0%
30	**Security risk management documentation** for regulatory submissions	100%	0%	0%
4	**Security requirements** for the product under development	100%	0%	0%
9	**Security architecture** providing the security context and trust boundaries of a medical device system	100%	0%	0%
11	**Post-market surveillance system** including cybersecurity considerations	98%	2%	0%
19	**Security risk assessment of post-market vulnerabilities**	98%	2%	0%
24	**Security risk management artifacts** (e.g., security risk management plan, security risk analysis, security risk management report, etc.)	98%	2%	0%
35	**Patch management process** for providing post-market security patches and updates	98%	2%	0%
13	**Product security incident response process**	96%	4%	0%
18	**Qualified and trained personnel** performing security risk management tasks	96%	4%	0%
37	**Security risk assessment of third-party software/firmware components** incorporated within a product	96%	4%	0%
6	**Vigilance process** for reporting serious incidents and field safety corrective actions related to cybersecurity incidents	96%	4%	0%
33	**Integrated security risk management process with accompanying processes** such as vulnerability handling, vulnerability disclosure, incident response, etc.	94%	6%	0%
23	**Security assessment of unresolved software anomalies** that exist in a product at the time of regulatory submission	92%	6%	2%
36	**Vulnerability management process**	92%	6%	2%
40	**Vulnerability management plans**	90%	10%	0%
10	**Monitoring of regulatory changes and developments** in cybersecurity laws, regulations, standards, and guidances for medical devices	88%	12%	0%
15	**Monitoring of cybersecurity information sources** to identify and detect potential security threats and vulnerabilities that may affect medical devices	88%	12%	0%
39	**Coordinated vulnerability disclosure process**	88%	12%	0%
14	**Labeling** to communicate relevant security information to users of medical devices	88%	10%	2%
5	**Threat modeling process**	88%	10%	2%
29	**Integrated security risk management process into a quality (management) system**	86%	14%	0%
26	**Premarket security testing** to identify and address potential vulnerabilities prior to exploitation	86%	12%	2%
8	**Software Bill of Materials (SBOM)**	84%	14%	2%
31	**Organizational roles and responsibilities** for security risk management	78%	22%	0%
32	**Post-market periodic security testing**, including penetration testing	78%	22%	0%
7	**Secure product development training for employees**	78%	20%	2%
38	**Internal/quality audits** of the security risk management program	73%	27%	0%
34	**Measures and metrics** for processes that reduce the number and severity of vulnerabilities in products	69%	31%	0%

Card #	Card name	Category		
		Required	Optional	Not necessary
2	**A dedicated team of product security professionals**	67%	31%	2%
20	**Software tools** to support security risk management tasks	33%	65%	2%
12	Medical device manufacturers participation in a health focused **Information Sharing Analysis Organization (ISAO)**	31%	59%	10%
16	**Security training for users** of medical devices	37%	55%	8%
28	**Glossary of terms and definitions** relating to medical device cybersecurity	41%	51%	8%

At the end of the card sorting exercises, the survey participants were asked to provide information what key elements of the security risk management program for medical devices are missing in the survey and to share any other thoughts about the security risk management. 7 of 53 respondents (13.2%) answered that no key elements are missing.

The following comments list the missing key elements according to the respondents:

- "Relevant Standards and Guidances"
- "Perhaps a specific register of cybersecurity regulations / standards that is used to define requirements for TPLC activities."
- "Check of regulatory requirements fulfilled"
- "secure design best practices, secure coding standards and their enforcement (e.g. code reviews, SAST), security event monitoring (for certain product types) if not already covered by PMS, software configuration management, release artifact archiving, security of IT infrastructure used for product/software development, test, production, delivery…, security of software distribution and software updates security (code integrity and security of code signing keys), supply chain security risk management (beyond assessment of 3rd-party components)"
- "Threat Modeling, Risk Management System, Risk Management Score, supply chain"
- "Security risk scoring, prioritisation, treatment of risk whether eliminated, mitigated, accepted or transferred."
- "evaluation of security risk with potential safety impact, legacy device security risk managment, product security continue support plan including retirement and obsolescence"
- "alignment with IEC14971 and Patient risk management process"
- "Who and how to connect security risks with safety."
- "Design Reviews, Digital Signature handling (File Integrity and Private Key Protection)"
- "Cryptography / protocol design considerations. It's a bad idea to "roll your own" or even implement your own instead of using a library, but correct library usage should still be monitored, the correct choice of algorithms and key lengths should be as well, and if implementing your own for whatever reason, a cryptography exert should be consulted on the protocol design and a cryptography implementation expert should be consulted on implementation details."
- "…Only suggestion would be to differentiate between pre- and post-market risk and vulnerability management. Although there is some overlap there are also some very specific differences with pre-market being more tied in with engineering processes whereas post-market being more about customer communication and management. Also, there was a question about post-market pen testing. I would see pen testing more as a pre-market activity, although one could make the argument of periodically repeating certain assessment activities. So ... I am not necessarily disagreeing, just wanted to clarify."
- "Multi-year architecture strategy to prepare for long product life, SBOM based monitoring for new vulnerabilities in post-market, Strategy for secure connectivity over Internet"
- "SLAs"
- "…Penetration testing wasn't covered"
- "Maybe clearly identify penetration and fuzz testing and software composition analysis."
- "The first section differentiated between qualitative and quantitative risk severity assessments, but I think it could have been mentioned in the following two sections."

The following key elements of the security risk management program for medical devices were mentioned by respondents as missing, but they were present in the card set:

- threat modeling (card #5);
- secure design best practices, secure coding standards, code reviews, software configuration management, design reviews, and security of IT infrastructure are best practices for a secure product development life cycle/framework (card #1);
- connecting security risks with safety, evaluation of security risk with potential safety impact, alignment with ISO 14971 (*ISO 14971: Medical devices – Application of risk management to medical devices*, 2019) and patient risk management process, legacy device security risk management, security risk scoring, risk management score, prioritisation, and security risk control options are associated with the security risk management process (card #3);

- penetration and fuzz testing were implicitly covered (card #26);
- penetration testing was explicitly covered (card #32);
- SBOM based monitoring for new vulnerabilities needs to be conducted during both premarket and post-market phases (card #25);
- differentiation between premarket and post-market risk management (card #19, #21);
- vulnerability management (card #11, #36, #39, #40).

Relevant cybersecurity standards and guidances were not written on the individual card #27 on purpose to keep it concise. Some key elements were mentioned as missing (e.g., security event monitoring, cryptography, code integrity, file integrity, secure software updates), but they are examples of security risk controls (card #17). Each manufacturer can choose its approach for performing a security risk assessment (e.g., quantitative, etc.) and the label of card #21 did not contain this information. One respondent mentioned a service-level agreement (SLA) which is a contract between the service provider (e.g., medical device manufacturer) and the customer (e.g., health delivery organization). Such agreement may contain specific security requirements that may not be considered during design and development. Supply chain risk management was also missing in the card set.

The following comments list the thoughts about the security risk management from the respondents:

- "follow some guidelines TIR57, NIST RMF, NIST CSF"
- "The security risk management should be implemented as a part of the overall product and process risk management"
- "It was hard for me to separate security risk management from total product lifecycle. For me, the latter includes the first ;-)"
- "When asked to categorize stuff under "most appropriate" labels, there were a number of items that were either detail-dependent (e.g. nature of the product) and/or fit equally well into two or more labels."
- "Security risk management and product security governance may all form a combined organization. The main decision point for certain aspects, like a dedicated team of experts central vs dispersed in product organizations entirely depends on the company and their ability to maintain expertise dispersed but consistent. There is no standard most effective model; key is for all elements of the program to be present, consistent and coordinated."
- "Contracts are a very important aspect of system security."
- "The current methodology is still very confusing and difficult to implement, especially for medical devices that privacy/data protection is also involved."
- "Risk transfer is a key element, in case a risk cannot be handled at manufacturer. Risk should not be accepted on behalf of end customer. Risk transfer along with suggestions to address the risk at user's end should be well documented."
- "Security controls should be appropriate for the risk introduced by the device into the system it will operate in and the function it performs. This may be best achieved by isolating clinical control from external comms to the maximum extent possible"
- "There is a serious gap in subject matter experts when it comes to cybersecurity in medical devices, most people think of corporate cybersecurity and not product security which leads to gaps in knowledge when trying to hire."
- "…I think we are all waiting to see what, if any, risk considerations greater AI integration in medical devices will bring. In the US the FDA rapidly advancing the regulatory criteria and it is something that is important to keep an eye on."

5 Conclusion and Future Work

This paper presents the use of the closed card sorting technique to classify 40 elements of the security risk management program for medical devices. The study used individual card sorting and involved a total of 40 cards. Every card had a name which represented an element of the security risk management program for medical devices. The analysis of closed card sort data and collected qualitative data was useful to elicit knowledge and to find out how the practitioners would distribute the cards within the predefined categories. Card sorts were helpful to better understand the connection between categories and various elements of the security risk management program for medical devices, and to determine which elements are suitable, missing, or need improvement.

LinkedIn professional network can be used to identify and recruit qualified participants for the survey. LinkedIn profiles provide valuable information about members, including their job title, location, industry, and experience, all of which are publicly available. When recruiting a large number of potential participants, a LinkedIn Premium account is required to browse for profiles without limits and to use InMail messages to directly message another LinkedIn member that you are not connected to.

When conducting an online survey research that addresses sensitive topics such as cybersecurity of medical devices, it is recommended to use an anonymous survey. The respondents will feel freer and more comfortable raising their concerns and giving honest, detailed answers with no inhibitions.

When using online surveys, it is recommended to use security survey options afforded by the tool (e.g.,

bot detection, preventing multiple submissions by the same person, preventing security scanners from accidentally starting a new session on the survey, etc.). While convenient and efficient, online surveys are subject to security concerns (e.g., survey scams, phishing links) from the potential survey participants, especially when the recipients of a survey link don't know the person who sent the link.

Card sort results and qualitative data including respondent comments will be considered when designing a new conceptual framework for managing security risks of medical devices. Categorizing with overlapping categories needs further investigation.

Acknowledgments

The author extends their gratitude to the survey participants, the reviewers of the survey, and the anonymous reviewers of the paper for their invaluable support of the research.

References

AAMI TIR57: Principles for medical device security–Risk management. (2016).

AAMI TIR97: Principles for medical device security–Postmarket risk management for device manufacturers (2019).

ANSI/AAMI SW96: Standard for medical device security–Security risk management for device manufacturers. (2023).

Barrett, A.R. & Edwards, J.S. (1995). Knowledge elicitation and knowledge representation in a large domain with multiple experts. Expert Systems with Applications, 8(1), 169–176.

FDA. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/86174/download

FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/95862/download

FDA. (2022). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions – Draft Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/119933/download

FDA. (2023). Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/166614/download

Fincher, S. & Tenenberg, J. (2005). Making sense of card sorting data. Expert Systems, 22(3), 89–93.

Hrgarek Lechner, N. (2021). The Key Elements of a Risk-based Product Security Program for Medical Devices: A Scoping Study. In N. Vrček, E. Pergler, & P. Grd (Eds.), Proceedings of the 32nd Central European Conference on Information and Intelligent System (CECIIS 2021) (pp. 257–264). University of Zagreb, Faculty of Organization and Informatics Varaždin.

IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle. (2021).

ISO 14971: Medical devices – Application of risk management to medical devices. (2019).

Lantz, E., Keeley, J. W., Roberts, M. C., Medina-Mora, M. E., Sharan, P., & Reed, G. M. (2019). Card sorting data collection methodology: How many participants is most efficient?. Journal of Classification, 36(3), 649–658.

Medical Device Coordination Group. (2020). MDCG 2019-16 Rev. 1 Guidance on Cybersecurity for medical devices. Retrieved from https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

Nielsen, J. (2004, July 18). Card Sorting: How Many Users to Test. Nielsen Norman Group. https://www.nngroup.com/articles/card-sorting-how-many-users-to-test/

Ray, A. (2021). Cybersecurity for Connected Medical Devices. Eastbourne: Academic Press.

Rugg, G. & McGeorge, P. (1997). The sorting techniques: a tutorial paper on card sorts, picture sorts and item sorts. Expert Systems, 14(2), 80–93.

Spencer, D. (2009). Card sorting: Designing usable categories. New York: Rosenfeld Media.

Tullis, T. & Wood, L. (2004, June 7–11). How Many Users Are Enough for a Card-Sorting Study? [Conference paper]. Usability Professionals Association (UPA) 2004 Conference, Minneapolis, MN, United States.

U.S. Department of Health and Human Services. (2013, October) Card Sorting. https://www.usability.gov/how-to-and-tools/methods/card-sorting.html

Wirth, A., Gates, C., & Smith, J. (2020). Medical Device Cybersecurity for Engineers and Manufacturers. Boston: Artech House.