Supporting lay bystanders during medical emergencies – risk assessment of video calls for emergency dispatch

Stein R Bolle*[1,2], Per Hasvold[1] and Eva Henriksen[1]

[1]Norwegian Centre for Integrated Care and Telemedicine, University Hospital of North Norway, N-9038 Tromsø, Norway
[2]Division of Trauma Care and Pre-Hospital Services, University Hospital of North Norway, N-9038 Tromsø, Norway

Email: Stein R Bolle*- stein.roald.bolle@telemed.no; Per Hasvold - per.hasvold@telemed.no; Eva Henriksen - eva.henriksen@telemed.no;

*Corresponding author

Abstract

Background: Video calls from mobile phones can improve communication during medical emergencies. Lay bystanders can be instructed and supervised by health professionals at Emergency Medical Communication Centers. Before implementation of video mobile calls in emergencies, issues of information security should be addressed.

Methods: Information security was assessed for risk based on the information security standard ISO/IEC 27005:2008. A multi-professional team used structured brainstorming to find threats to the information security aspects confidentiality, quality, integrity, and availability.

Results: Twenty security threats of different risk levels were identified and analyzed. Solutions were proposed to reduce the risk level.

Conclusions: Given proper implementation, we found no risks to information security that would advocate against the use of video calls between lay bystanders and these call centers. The identified threats should be used as input to formal requirements when planning and implementing video calls from mobile phones for Emergency Medical Communication Centers.

Supporting lay bystanders during medical emergencies – risk assessment of video calls for emergency dispatch

Stein R Bolle*[1,2], Per Hasvold[1] and Eva Henriksen[1]

[1]Norwegian Centre for Integrated Care and Telemedicine, University Hospital of North Norway, N-9038 Tromsø, Norway
[2]Division of Trauma Care and Pre-Hospital Services, University Hospital of North Norway, N-9038 Tromsø, Norway

Email: Stein R Bolle*- stein.roald.bolle@telemed.no; Per Hasvold - per.hasvold@telemed.no; Eva Henriksen - eva.henriksen@telemed.no; Stein R Bolle*- stein.roald.bolle@telemed.no; Per Hasvold - per.hasvold@telemed.no; Eva Henriksen - eva.henriksen@telemed.no;

*Corresponding author

Background

Cardiac arrest, accidents and traumas are leading causes of death worldwide [1, 2]. First rescue activities done by lay bystanders, such as calling for help, opening of airways, and cardio-pulmonary resuscitation, save lives. Emergency Medical Communication Centers (EMCCs) assist bystanders via telephone, saving time and improving care. EMCC operators (dispatchers) often have to act on limited information, as the description given by bystanders can be lacking or misleading [3–5].

Videoconference enabled mobile phones can be sophisticated tools for dispatcher assisted resuscitation [5, 6], and videoconferencing can improve the confidence of lay rescuers [7]. If videoconferencing is used in communication between bystanders and EMCCs, dispatchers would be able to see the patient, the scene of accident, and may better instruct bystanders on correct action [5, 8, 9]. The Federal Communications Commission (FCC) in the USA announced in November 2010 that America's 9-1-1 system should be revolutionized by harnessing the life-saving potential of text, photo, and video in emergencies [10]. Although a majority of the emergency calls come from mobile phones, call centers lack the technical capability to use the full potential of these new technologies.

In healthcare, information security and safety are vital parts of the trust between the public and the care providers. In most countries this is regulated through laws and professional standards. Before the implementation of video calls in EMCCs, possible undesired effects should be identified. In this study, the security challenges of using mobile telephones for videoconferencing between lay rescuers and EMCCs were analyzed through a qualitative risk assessment of the information security aspects.

Methods

Risk assessment is a systematic approach for describing and calculating risks of undesired events. We conducted risk assessment of information security related to the use of videoconference calls with mobile phones between lay bystanders and EMCCs during medical emergencies. Our risk assessment was based on the information security standard ISO/IEC 27005:2008 developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [11]. In this standard, risk assessment is described as a process consisting of risk identification, risk estimation and risk evaluation. Risk assessment is performed after context establishment, and the process may be iterative (Figure 1).

Risk assessment group, workflow and time frame

Risk assessment was performed by a group, led by a risk assessment expert (EH). Group participants were chosen from our own institution, based on competencies and background, such that different areas of expertise were covered. One nurse, one physician, one lawyer, and two computer scientists took part in this group, which started its work in 2006. After one iteration of risk assessment including three group meetings, we found that a better understanding of the intended service was needed, and agreed to postpone further iterations to the completion of a research project [5, 12]. We expanded our group with a dispatcher nurse who had tested the technology, and the risk assessment was completed through another two iterations with email discussions and eight group meetings during 2009 and 2010.

Context establishment

The context for this risk assessment was set by describing the service, legal requirements and definitions. Legal requirements for communication of sensitive patient-identifiable information is set by national and European legislation [13–15]. The consequence of risks were defined in three categories (low, medium, high), and values for likelihood were described using four categories (low, medium, high, very high) (Table 1). Risk (R) is the product of consequence (C) and likelihood (L): R = C * L. We defined three levels for risks; low, moderate and severe (Table 1). Threats with severe risk are usually unacceptable. If they cannot be avoided or their risk reduced, it may imply that the new service should not be implemented.

Risk assessment

Threats with consequences for the organization or patients were identified. We considered threats regarding legislation and regulations, economic consequences, reputation, life, and health. Risk assessment was done for the new service relative to the existing service with audio only communication. This means that risks in the existing service were excluded, unless the new service would change the risk level.

Identification of threats to information security was performed as a structured brainstorming in the risk assessment group. All ideas for possible risks were noted and no risks were censored or rejected at this point. During risk assessment we focused on confidentiality (c), quality (q), integrity (i), and availability (a) of information, terms defined by Norwegian legislation as the aspects of information security [13, 14]. Every threat was described and given a unique id where the first character was used to indicate the type of security aspect (c, q, i, a).

Each threat was analysed by the team for the consequence and the likelihood that it would occur, according to definitions (Table 1). Threats with no likelihood of occuring or no consequence were not followed further. The risk level was illustrated as a combination of consequence and likelihood in a two dimensional matrix.

The risk level of each threat was evaluated, and possible actions to reduce the risks were suggested.

Results

Twenty distinct threats and unwanted situations were identified and described (Table 2). The likelihood and consequence were estimated for each threat. The risk matrix presents all threats with their id, short description and risk level as a combination of likelihood and consequence (Figure 2). No threats had a severe risk level, but threats with a high level of consequence should be watched closely, as an increase in likelihood can make these threats severe. We were not able to conclude on likelihood or consequence for nine threats, either because it would be dependent on the implementation of the technology, or related to issues that can only be answered through clinical trials. In the worst case, these threats could have an unacceptable severe risk.

Different options for risk treatment were suggested. Several threats can be removed by proper implementation: the lack of availability of video logs (a3, a4, a5), the inability to forward video calls (a9), and unauthorized access to patient information (c2, c3). The loss of dispatchers' identity protection (m1) can be avoided with one-way videoconferencing, or by transmitting computer generated images of a dispatcher (an avatar) [16].

Some threats will be influenced by the intellectual capacity of dispatchers. Training of dispatchers may reduce the risk level of those threats, such as poor image quality (q2), misunderstandings due to interpretation of images or several patients in the same emergency (q3, q4, q5), and the images receiving too much attention from dispatchers or bystanders (m2, m3). For some dispatchers and in some situations the image may be helpful, while at times images can be an extra burden. EMCCs commonly use criteria based protocols for advice during emergencies [17–19]. Such protocols should be adapted for video based dispatch [5, 12], which may contribute to reduction of the risk level for these threats.

The risk level of the remaining threats will be largely influenced by factors external to EMCCs, such as the sound quality (q1), time delays when establishing videoconferencing (a1), the capacity and security of the telecommunication networks (a2, a7, c1), weather conditions (a6), and the quality and capacity of callers' mobile phones (a7, a8). The risk level of these threats are likely to decrease with time, as technology and solutions mature. If users experience problems with sound quality or other technical problems during a video call, a switch to audio call may solve the problem, but with a time cost.

Discussion

This risk assessment identified twenty threats to information security for the use of mobile video calls between Emergency Medical Communication Centers and the public. None of these have a severe risk level (i.e., a combination of high consequence and likelihood). We have suggested ways to decrease or eliminate the risks, by proper implementation, organization, and staff training. Potential delays and poor sound quality were the greatest technical risks of mobile video calls. These threats are likely to decrease as technology improves.

Based on this risk assessment, we believe it is possible to implement videoconferencing from the public as a service in Emergency Medical Communication Centers with acceptable risks. However, some critical success factors of information systems in the organization are only discovered during the implementation process [20]. A change in work environment may impose unacceptable loads on human cognitive abilities and potentially lead to errors, especially in a transition phase when new routines are being adopted [21]. When introducing a new service in the high stress environment of Emergency Medical Communication Centers, the process should therefore be closely monitored for unwanted incidents, even if unacceptable risks have not been identified at earlier stages. Risk assessment should be repeated at regular intervals to ensure that changes in environment, organization, or system does not introduce new unacceptable threats and that known threats do not increase in likelihood or consequence resulting in unacceptable risk levels for the system.

The result of risk assessments provides information for risk treatment (Figure 1), which involves decisions on how to reduce risk in an organization. The threats identified in this risk assessment should be used as input to formal requirements when planning and implementing video calls for Emergency Medical Communication Centers. The benefit of doing risk assessment before system implementation is that information security can be incorporated from the beginning.

ISO/IEC 27005:2008 outlines procedures for risk assessment, but several of the steps can be addressed by using different approaches. We used qualitative assessments by a multi-professional team. The composition of the team is important to cover different threats, but is no guarantee that all possible threats are found. Similar to SWIFT, our approach was prospective and addresses a future system at a high level [22, 23]. Other methods for risk identification such as HAZOP, FMEA, and FTA focus on process flow or hardware, and may be better suited for assessment of equipment details [22].

A threat may have different outcomes, from common incidents with no practical implications, to (very rarely) a chain of events with disastrous results. Poor sound quality, for instance, may be acceptable in many situations, but can in other cases cause misunderstandings that lead to worse patient treatment and possible patient death. Assessment of consequence and likelihood associated with threats of a new service is therefore difficult when no numbers exist to support the estimations. We found this led to a worst-case type of thinking that may have overestimated the risk level of some threats. Further studies are therefore needed to map type of errors and problems that may arise when videoconferencing is used during real emergencies.

Conclusions

Video based communication with lay bystanders during prehospital emergencies may potentially improve the quality of prehospital patient care. In previous studies of simulated cardiac arrest, we have found that video calls are likely to improve confidence and reduce communication problems during prehospital medical emergencies [5, 7]. In this risk assessment, we used qualitative methods to find potential threats to information security of using such video calls. This study has revealed several issues that should be considered carefully in requirement specifications for such systems. We did not identify potential threats with unacceptable high risk levels, which indicates that it is possible to implement the reception of video calls from the public in dispatch centers. The time is ripe to start to discuss how emergency call centers should implement the new possibilites given by the mobile multi-media devices carried by a large portion of the population.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

SRB conceived of the study, and participated in its design and coordination, took part in the risk assessment group and drafted the manuscript. PH participated in the design of the study, took part in the risk assessment group and helped to draft the manuscript. EH participated in the design and coordination of the study, was leading the risk assessment and helped to draft the manuscript. All authors read and approved the final manuscript.

Authors' information

SRB is an anesthesiologist (MD) with a background in computer science. PH is a computer scientist. EH is an expert on risk assessment with a background in computer science.

Acknowledgements and Funding

The authors acknowledge Oddvar Hagen, Mona Hagensen, Leif Erik Nohr and Jeremiah Scholl for their participation in the risk assessment group.

The study was supported by grants from The Northern Norway Regional Health Authority through the Committee for Telemedicine Research Programme. Role of the funding body: None.

References

1. Murray CJ, Lopez AD: **Mortality by cause for eight regions of the world: Global Burden of Disease Study.** *Lancet* 1997, **349**(9061):1269–1276, [http://dx.doi.org/10.1016/S0140-6736(96)07493-4].

2. Krug EG, Sharma GK, Lozano R: **The global burden of injuries.** *Am J Public Health* 2000, **90**(4):523–526.

3. Forslund K, Kihlgren A, Kihlgren M: **Operators' experiences of emergency calls.** *J Telemed Telecare* 2004, **10**(5):290–297.

4. Tjora A: *Calls for Care. Coordination, compentence, and computers in medical emergency call centres.* VDM Verlag Dr. Müller 2009.

5. Johnsen E, Bolle SR: **To see or not to see – Better dispatcher-assisted CPR with video-calls? A qualitative study based on simulated trials.** *Resuscitation* 2008, **78**(3):320–326.

6. Morley P: **Video instruction for dispatch-assisted cardiopulmonary resuscitation: two steps forward and one step back!** *Crit Care Med* 2009, **37**(2):753–754.

7. Bolle SR, Johnsen E, Gilbert M: **Video calls for dispatcher-assisted cardiopulmonary resuscitation can improve the confidence of lay rescuers - surveys after simulated cardiac arrest.** *J Telemed Telecare* 2010, [http://dx.doi.org/10.1258/jtt.2010.100605].

8. Yang CW, Wang HC, Chiang WC, Chang WT, Yen ZS, Chen SY, Ko PCI, Ma MHM, Chen SC, Chang SC, Lin FY: **Impact of adding video communication to dispatch instructions on the quality of rescue breathing in simulated cardiac arrests–a randomized controlled study.** *Resuscitation* 2008, **78**(3):327–332.

9. Yang CW, Wang HC, Chiang WC, Hsu CW, Chang WT, Yen ZS, Ko PCI, Ma MHM, Chen SC, Chang SC: **Interactive video instruction improves the quality of dispatcher-assisted chest compression-only cardiopulmonary resuscitation in simulated cardiac arrests.** *Crit Care Med* 2009, **37**(2):490–495.

10. Federal Communications Commission: **Chairman Genachowski Announces Steps to Bring 9-1-1 into 21st Century.** *http://www.fcc.gov/headlines2010.html.*

11. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC): **ISO/IEC 27005:2008, Information Technology – Security Techniques – Information Security Risk Management** 2008. [1st edition 2008-06-15.].

12. Bolle SR, Scholl J, Gilbertz M: **Can video mobile phones improve CPR quality when used for dispatcher assistance during simulated cardiac arrest?** *Acta Anaesthesiol Scand* 2009, **53**:116–120.

13. **Norwegian Act of 14 April 2000 no. 31 relating to the processing of personal data [Personal Data Act]**[http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf].

14. **Norwegian Act of 18 May 2001 no 24 on personal health data filing systems and the processing of personal health data [Personal Health Data Filing System Act].**[http://www.ub.uio.no/ujur/ulovdata/lov-20010518-024-eng.pdf].

15. European Parliament and Council of the European Union: **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data** 24 Oct 1995, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML].

16. Kang S, Watt J, Ala S: **Social copresence in anonymous social interactions using a mobile video telephone**. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, ACM 2008:1535–1544.

17. Cheung S, Deakin CD, Hsu R, Petley GW, Clewlow F: **A prospective manikin-based observational study of telephone-directed cardiopulmonary resuscitation.** *Resuscitation* 2007, **72**(3):425–435, [http://dx.doi.org/10.1016/j.resuscitation.2006.07.025].

18. Roppolo LP, Pepe PE, Cimon N, Gay M, Patterson B, Yancey A, Clawson JJ, Council of Standards Pre-Arrival Instruction Committee NAoEDwg: **Modified cardiopulmonary resuscitation (CPR) instruction protocols for emergency medical dispatchers: rationale and recommendations.** *Resuscitation* 2005, **65**(2):203–210.

19. The Laerdal Foundation for Acute Medicine: **Norsk indeks for medisinsk nødhjelp. 2nd ed.** *Den norske lægeforening.* Stavanger 1999.

20. Berg M: **Implementing information systems in health care organizations: myths and challenges.** *Int J Med Inform* 2001, **64**(2-3):143–156.

21. Parker J, Coiera E: **Improving clinical communication: a view from psychology.** *J Am Med Inform Assoc* 2000, **7**(5):453–461.

22. Aven T: *Risk analysis: assessing uncertainties beyond expected values and probabilities*, Wiley 2008 chap. Risk analysis methods, :57–84.

23. Smith A, Boult M, Woods I, Johnson S: **Promoting patient safety through prospective risk identification: example from peri-operative care.** *Qual Saf Health Care* 2010, **19**:69–73, [http://dx.doi.org/10.1136/qshc.2008.028050].

24. Eisenberg MS, Hallstrom AP, Carter WB, Cummins RO, Bergner L, Pierce J: **Emergency CPR instruction via telephone.** *Am J Public Health* 1985, **75**:47–50.

Figures

Figure 1: The workflow of risk assessment according to the information security standard ISO/IEC 27005:2008.

Figure 2: Risk matrix presenting the identified threats with id and short description. Darker shades of grey indicates higher level of risk: light grey low risk, medium grey moderate risk and darkest grey severe risk. White background is used for threats with unknown risk.

Table 1: **Definitions of consequence, likelihood and risk level**

Category	**Description**
	Consequence
Low	For the hospital or the service: No violation of law; or negligible economic loss which can be restored; or small reduction of reputation in the short run. For the patient: A minor impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run.
Medium	For the hospital or the service: Offence, less serious violation of law which results in a warning or a reprimand; or economic loss which can be restored; or reduction of reputation that may influence trust and respect. For the patient: A minor temporary impact on health; or economic loss which can be restored; or small reduction of reputation caused by revealing of less serious information (e.g. blood pressure level).
High	For the hospital or the service: Violation of law which results in penalty or fine; or a large economic loss which cannot be restored; or serious loss of reputation that will influence trust and respect for a long time. For the patient: Death or permanent reduction of health; or a large economic loss which cannot be restored; or serious loss of reputation caused by revealing of sensitive and offending information.
	Likelihood
Low	Rare, occurs less than every 100th connection. Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately.
Medium	May happen, occurs between every 10th and every100th connection. Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.
High	Quite often, occurs between every 3rd and every10th connection. Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
Very high	Very often, occurs more often than every 3rd connection. Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
	Risk level
Low	Acceptable risk. The service can be used with the identified threats, but the threats must be observed to discover changes that could raise the risk level.
Moderate	Can for this service be an acceptable risk, but for each threat the development of the risk should be monitored to consider whether necessary measures have to be implemented.
Severe	Not acceptable risk. Cannot start using the service before risk reducing treatment has been implemented.

Table 2: Description of threats

Threat id	**Description**
	Threats to quality
q1	Sound quality with mobile phone videoconferencing is usually worse than regular calls between mobile phones. Reasons include poor bandwidth and mobile phones usually in loudspeaker mode during video calls, often with disturbing background noise. This may result in misunderstandings, lost information and delays.
q2	Poor image quality is a common problem with video calls from mobile phones. Although likely to improve with improved technology, camera shake, poor light and weather conditions will influence on the image quality. Some image quality problems are due to current methods for video compression.
q3	The caller may believe that the image is a sufficient description, therefore not describing the situation appropriately, which leads to misinterpretations.
q4	the dispatcher may believe the image describes the situation sufficiently, and therefore do not ask for important information, which leads to misinterpretations.
q5	When there are several patients in the same accident or emergency, it is possible to mix-up images from one patient to what is said about another patient. The image may clarify or complicate matters when much information needs to be sorted out.
	Threats to availability
a1	It usually takes more time to establish a phone call with video. Today this is usually a matter of a few seconds, time which may be saved in successful guidance trough video communication. The caller may however be negatively affected by delays during initiation of contact with the EMCC, which in turn may affect how the case is handled.
a2	The capacity of mobile phone networks is often reached during larger accidents. videoconferencing demands more bandwidth than audio communication, which may be a problem when many people are calling at the same time. In some mobile networks video calls use a reserved bandwidth, not interfering with the bandwidth used for audio calls. Depending on traffic and network configuration, it can be easier or more difficult to make a call go through when using video calls.
a3, a4, a5	EMCCs commonly have audio logs of all communication with the public for playback. If the connection with the caller is lost and cannot be reestablished, audio playback may provide essential information to solve the emergency. Audio logs can also be useful for debriefing, or when questions later arise if the EMCC should have handled a case differently. If, for some reason, the log is not available, it may negatively affect patients in cases where connection is lost (threat a3). It may negatively influence the organization if logs are not available for documentation (threat a4) or debriefing (threat a5). There are several causes for these threats to occur, either that video is not recorded by default implementation, that playback of videorecordings is difficult, or that such recordings are corrupted or destroyed.
a6	Mobiles used for videoconferencing is kept out from the body and has greater exposure to weather conditions such as rain and cold temperatures. This may cause equipment failure and loss of connection.
a7	Technical difficulties because of less stable connection during mobile videoconferencing can delay or disrupt the exchange of information.
a8	Videoconferencing drain more battery on mobile phones than does audio communication. Use of video may therefore cause more lost connections. With empty batteries, communication can not be reestablished.

Continued on Next Page...

Table 2 – Continued

Threat id	Description
a9	In some situations the dispatcher may want to forward the call to another dispatcher either within the same EMCC or in a different EMCC. If this is not possible during video calls, the dispatcher may shut down the call and establish an audio call instead. This comes with a risk of wasting time.
Threats to confidentiality	
c1	Telephone communication can be wiretapped. While it takes more advanced technology and skills to wiretap a live videoconference over a mobile network, the public interest in images from emergencies suggest increased willingness to invest in such technology.
c2	Stored images are likely to be of greater interest and may contain more sensitive patient information than audio logs. Stored video and images may therefore increase attempts of unauthorized access.
c3	If visitors are allowed into the EMCC, or the images on computer screens can be observed by people outside the EMCC, this may reveal patient sensitive information. This threat is dependent on local conditions such as placement of computer screens and access restrictions to the EMCC.
Threats to integrity	
	No threats to data integrity were identified.
Mixed threats	
m1	With two-way videoconferencing the caller may identify the dispatcher. Dispatchers have been concerned that the loss of identity protection makes them more vulnerable to insults [5].
m2	The EMCC is a demanding work environment, and the introduction of videoconferencing may distract or increase demands on dispatchers. In the worst case, this may cause inefficiency or delays.
m3	The caller may focus on filming rather than helping the patient. The dispatcher may ask for images, and disturb or interrupt the treatment the caller otherwise would have initiated. Similar concerns were also raised when resuscitation instructions first was provided by telephone [24].

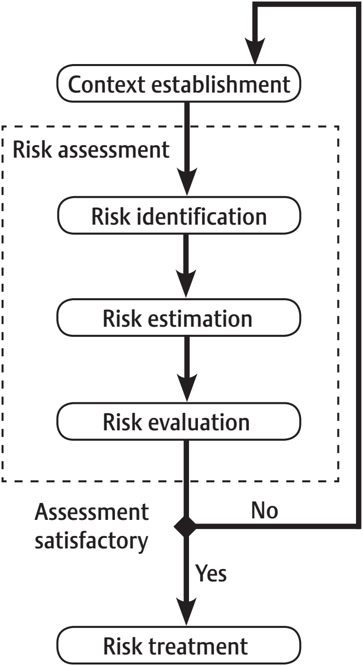
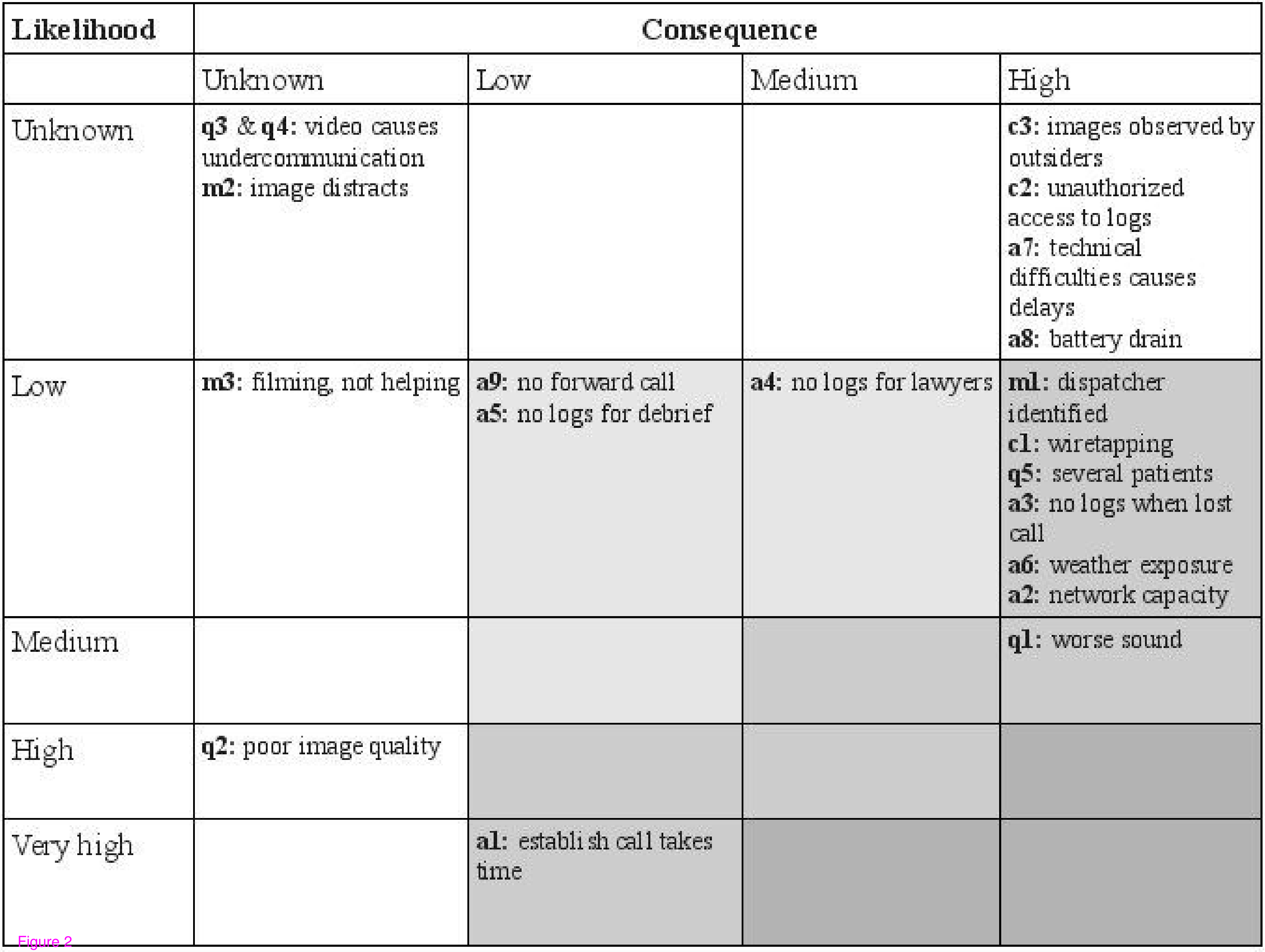

Context establishment
Risk assessment
Risk identification
Risk estimation
Risk evaluation
Assessment satisfactory
No
Yes
Risk treatment

Figure 1



Likelihood	**Consequence**			
	Unknown	Low	Medium	High
Unknown	**q3** & **q4**: video causes undercommunication **m2**: image distracts			**c3**: images observed by outsiders **c2**: unauthorized access to logs **a7**: technical difficulties causes delays **a8**: battery drain
Low	**m3**: filming, not helping	**a9**: no forward call **a5**: no logs for debrief	**a4**: no logs for lawyers	**m1**: dispatcher identified **c1**: wiretapping **q5**: several patients **a3**: no logs when lost call **a6**: weather exposure **a2**: network capacity
Medium				**q1**: worse sound
High	**q2**: poor image quality			
Very high		**a1**: establish call takes time		

Figure 2