Securing a collaborative information management system is divided between technical forms of security, such as firewalling and encryption, and social forms of security, such as trust. In order to properly provide security to a system, both aspects must be addressed in relation to each other, not one after the other or each one by separate committees. Even more, not having everyone on the same page about what security means and the responsibility to achieve and maintain it, can jeopardise the long-term security of a collaborative information management system.

Guiding Questions

Who is responsible for the collaborative platform's security? Technology? Designers? Responders? The host?

Where in the system is security maintained? Is it in the system architecture? The data links? The network? With the users? In the governance?

What is the purpose of the system's security? Supporting privacy? Sharing? Democratic deliberation?

When can security be guaranteed? When entering data? While data is stored? While it is used?

Are the three main goals of information security (availability, integrity, confidentiality) considered? If not, why not?

What is the relation between security and privacy or informational self-determination, i.e. the ability to decide what information about persons goes where?

Do the rules for security stay the same as data crosses boundaries?

Further Information

The security of collaborative information management systems entails the formation of a strategy of risk management which outlines who has responsibility for monitoring and implementing system security. Common security threats include: system failure, hacking, and infection. Most institutions and organisations already have guidelines and laws for managing such threats to a system. Other security risks to the system, however, include more organisational and collaborative aspects of CIS use, including information leaks and business models that do not adequately address the diverse needs of cross-border

interoperability. These threats to security, both technological and social, need to be clearly defined in order to be addressed when setting up the CIS, and re-evaluated regularly.

However, security becomes a much more complicated problem than simply keeping data out of the hands of those who do not have the rights to it. The question of who has the rights might change depending on socio-political context or the specific incident. As security is managed, it has to balance regulations, trade negotiations (who can have the data and at what expense), and intelligence collection (namely, what is the benefit of knowing and does it outweigh the risks?).

Security becomes an increasing challenge when dealing with social media and big data endeavours. For example, these latter tools can be used for monitoring patterns of certain users that may have been involved in some "odd" activity in order to try to determine the intentions of their actions, and, by combining social media use with their individual network 'signature', to determine risk to society. Here, security walks a fine line between surveillance, privacy, consent, pre-emptive risk assessment, and human dignity.

Security should also be transparent, especially when engaging with organizations outside formal response, to increase trust in these interactions.

Exampels

The terrorist attack at the Inland Regional Center in San Bernardino, California, in December 2015 that killed 14 people has highlighted how security is a challenge that needs to be negotiated between different actors in specific socio-political contexts.

When the FBI got hold of the iPhone of one of the attackers, they asked Apple's help to unlock it by building a 'backdoor' that would allow federal law enforcement agencies to access the device. Apple quickly refused – initially the request and later the court order – claiming that forcing it to create such software would violate the company's constitutional rights and weaken privacy for users around the world.

This is a contentious issue that urges us to consider practical questions such as 'should tech companies be obliged to guarantee government access to encrypted data on smartphones and other digital devices, and is that even possible without compromising the security of law-abiding customers? (Nakashima and Gellman 2015), but it is also a case that highlights the precarious balance between security and privacy, and the technological practices such as encryption that make these discussions pertinent.

Resources

Petersen, K. et al. (2015) ELSI guidelines for collaborative design and database of representative emergency and disaster. SecInCoRe Project EU Deliverable D2.02 [Link]

Büscher, M., Kuhnert, M., Pottebaum, J., Ahlsén, M., Easton, C., Van Veelen, B., and Wietfeld, C. (2014). Cloud Ethics for Disaster Response. *Proceedings of the ISCRAM Conference 2014* [Link]

Nakashima, E. and Gellman, B. (2015) As encryption spreads, U.S. grapples with clash between privacy, security, The Washington Post April 10, 2015 [Link]