Human Aspects of Security Collaboration

Tomas Sander
HP Labs
tomas.sander@hp.com

Introduction

The value of a security online sharing community depends on the usefulness of the information it makes available to its members and thus depends on the data members contribute. Many existing sharing efforts involve human participation, via email, portals or conference calls. Fortunately better tool support is becoming available. Nevertheless human effort is still needed. Sharing platforms are not (yet) fully integrated with the SOC environment, e.g. case management systems. Thus analysts have to cut and paste case data into a sharing tool. Incident reports, TTPs, insights on threat actors etc. are valuable data to share, yet this requires analyst work. The key suggestion of this paper is to study security information sharing (also) as a human behavior, complimenting the research on automated sharing. This allows to apply tools from behavioral sciences which leads to novel and interesting perspectives.

Applying a Model from Behavior Change Technologies

As a simple example we look at the Fogg Behavior Model (FBM) [1] which has been successfully used for building mobile health applications that encourage users to exercise more, eat better etc. The target behavior we wish to encourage is to contribute useful security related information to a community.

FBM asserts that "for a person to perform a target behavior, he or she must (1) be sufficiently motivated, (2) have the ability to perform the behavior, and (3) be triggered to perform the behavior" [1]. Motivation trades off with ability: a CSIRT analyst investigating a complex incident may create and share a description as she is highly motivated by the hope for feedback. Normally she may only be willing to upload a list of found threat indicator though if that's very easy to do as she has little to gain.

In order to make sharing more likely, this model suggests you can 1) increase motivation, 2) increase the ability to perform a behavior and 3) create triggers to alert the user to execute the behavior.

Let's look at these in turn. How can we increase *motivation*? Educating users that their sharing is important to the community (and therefore the right thing to do) is one way to increase motivation. Users will feel especially motivated if feedback is provided to them that the specific data *they* are providing is important. Another way to increase motivation is to increase utility, e.g. by automatically cross-correlating uploaded data with community data and to alert users if that turns up anything noteworthy, such as previous attacks. A few informal interviews with analysts suggest that getting the job done is not the only reason they like participating in sharing communities. They also value building closer relationships with their peers. Consequently sharing communities relying mostly on anonymous sharing may not motivate analysts as effectively as communities that also advance their social interests.

How can we increase the *ability* of users to share information? The most obvious approach is to design tools that make sharing easy and to integrate them with other tools analysts use. Cumbersome data-entry is not the only cost to sharing though. If an analyst is uncertain if sharing some piece of data violates privacy rules or puts her organization at risk resolving this uncertainty may carry significant

costs. Sharing communities have an interest in lowering this cognitive burden on their members. To achieve that it would be helpful if organizations establish clear policies when and how to share information (and when not to) and to train their analysts accordingly.

What are appropriate *triggers* for sharing? A first step towards answering this question is to identify criteria and contextual cues when an analyst should share data. One strategy might be to train analysts to recognize if these criteria are fulfilled for cases they are working on. Another strategy would be for case management systems and other tools to send reminders suggesting to share case data. If these reminders are timed intelligently or identify specific benefits of sharing the case data, even better.

Thus applying this basic behavior model leads to interesting and novel questions, such as:

1. Do analysts benefit from training for sharing and, if yes, what should such a training contain?
2. What are appropriate behavioral triggers for sharing data?

Other relevant work

There is other relevant work that is influenced by behavioral sciences. Kraut et al. [2] have identified design patterns that address common challenges of online communities, such as encouraging contributions, encouraging commitment to the community and how to deal with newcomers. These challenges also arise in security sharing communities.

Organizational psychologists recently began to study CSIRTs in [3]. Their discipline has tools to identify the knowledge, skills, and abilities (KSAs) that are required to do a job well. For multi-team scenarios they already identified "information-sharing skills, collaboration skills, and a preference for working with others" as crucial KSAs [3]. Importantly organizational psychologists also have resources to help employees "get better" at these KSAs. As these KSAs are likely to be useful in online sharing communities as well this raises the question if there are interventions within Organizational Psychology (e.g. trainings to improve KSAs) that promise to make online sharing communities more effective. In addition research on how to build trust between individuals would be highly relevant.

HCI work on gamification also fits the user-centered spirit of this inquiry. Is it possible (or desirable) to make security sharing communities more playful and engaging using techniques, such as badges, leader boards, progress bars, feedback (such as 'likes') etc.?

In conclusion this paper suggests that studying security information sharing as a human behavior offers new, promising approaches to make security sharing communities more successful.

References

[1] Fogg B. *A behavior model for persuasive design.* Persuasive '09; 4th International Conference on Persuasive Technology; April 26-29, 2009; Claremont, CA, USA. 2009.

[2] R. E. Kraut, P. Resnick, S. Kiesler, Y. Ren, Y. Chen, M. Burke, N. Kittur, J. Riedl, and J. Konstan. *Building Successful Online Communities: Evidence-Based Social Design.* The MIT Press, 2012

[3] Tiffani R. Chen, Daniel B. Shore, Stephen J. Zaccaro, Reeshad S. Dalal, Lois E. Tetrick, Aiva K. Gorab. *An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams.* IEEE Security and Privacy Magazine 01/2014; 12(5):61-67.