2016 International Conference on Collaboration Technologies and Systems

Sensemaking and Storytelling: Network Security Strategies for Collaborative Groups

Elizabeth Anne Watkins
Columbia University
New York, New York, USA
elizabeth.watkins@columbia.edu

Franziska Roesner
University of Washington
Seattle, Washington, USA
franzi@cs.washington.edu

Susan McGregor
Columbia Journalism School, Columbia University
New York, New York, USA
sem2196@columbia.edu

Byron Lowens
School of Computing, Clemson University
Clemson, South Carolina, USA
blowens@g.clemson.edu

Kelly Caine
School of Computing, Clemson University
Clemson, South Carolina, USA
caine@clemson.edu

Mahdi Nasrullah Al-Ameen
School of Computing, Clemson University
Clemson, South Carolina, USA
malamee@clemson.edu

EXTENDED ABSTRACT

Networked organizations must grapple with a constant trade-off between ease of workflow for their employees, and devoting time and resources to computer security. In a group of collaborators whose workflows can differ substantially, creating broad and cohesive awareness around security can be difficult, especially for spaces like news institutions, where continuous collaboration must be carried out under continuous threat of cyberattack. Using a sensemaking framework, we analyzed interviews with two levels of organizational actors, lower-level reporters and higher-level supervising editors. Fragmented sensemaking, in which individuals maintain their own discrete and disconnected approaches to the complex situation of computer security, was pervasive. Storytelling as a sensemaking strategy, however, was found in both levels. In particular, while personal stories were shared by all participants, higher-level editors on average shared more second-hand narratives they'd heard about other organizations. Noting that editors described how such second-hand stories shaped their security decisions, we conclude with recommendations for integrating storytelling methods into robust training modules for computer security in collaborative working environments.

A. *Introduction*

Journalists are high-value targets for cyberattacks, including phishing, cyberspying, and surveillance [11, 3, 1, 6, 4, 7, 8]. Yet journalists must also rely on collaborative technologies, as their work is dependent on connections with sources, editors, and colleagues around the globe. Third-party software, such as document-sharing applications, cloud storage, content-management systems, and institutional email figure prominently in their work. In this highly-networked environment, the security behaviors of any single journalist can compromise their organization. News institutions need effective management strategies for training employees, many of whom are non-experts in computer security, to deal with a range of security threats.

Sensemaking is the process by which people give meaning to complex or chaotic experiences, and then use these structures of meaning to make decisions [5] a process well-suited to evaluating organizational computer security [10]. For example, institutional "sensegiving" (where high-level actors attempt to shape the perceptions and behaviors of lower-level employees) can include activities like holding meetings, conducting at-work training, and making recommendations for action. Lower-level "sensemaking" (where lower-tier employees discuss among themselves how best to comprehend and confront a situation) can include behaviors like seeking out expertise from social contacts, as well as storytelling [5].

While fewer than one-quarter of journalists in our study reported that their institutions had engaged them in security training or recommendations, we found that employees at engage in their own sensemaking behaviors. Storytelling was one prevalent strategy.

While personal experiences make individuals more conscious about security and privacy issues, compelling research

This work is supported in part by the National Science Foundation under Awards CNS-1513575, CNS-1513875, and CNS-1513663.

978-1-5090-2300-4/16 $31.00 © 2016 IEEE
DOI 10.1109/CTS.2016.118

has found that security stories people hear second-hand from people similar to themselves, i.e. friends and family, have greater impact on their security-related decisions than expert-led training modules or systems-based instruction [2]. This type of storytelling influences the behaviors of people who are not experts in computer security [9]. While prior work focused on domestic environments and analyzed user behaviors around home computers, our work seeks to analyze the potential of storytelling as a sensemaking strategy for organizational environments populated with non-experts in computer security. Second-hand stories, rather than personal accounts, can be more easily generalized to the larger population and into the design of robust training modules.

C. Methodology

We conducted in-depth, semi-structured interviews with 23 journalists about their computer security and information management practices in their professional work between late 2015 and early 2016. We then coded our transcribed interviews for "security stories": shared accounts of events related to issues in privacy or security. Examples include stories of phishing attacks, DDoS attacks, or cyberattacks by, for example, the Syrian Electronic Army. We also coded for stories of security-related actions that journalists had taken, including implementation of security tools such as two-factor authentication and encrypted chat programs. We coded these stories into two separate categories: personal stories of events that the storyteller had experienced directly, and "second-hand" stories stories of events the participants had heard about or reported on as part of their work. For our analysis of both first- and second-hand "security stories," we divided the number of stories told at a given organizational level by the number of participants at that level.

D. Results and Discussion

Our study revealed that higher-level organizational actors told second-hand stories at a higher average rate than lower-level actors. Supervising editors shared the highest number of second-hand stories per participant, while reporters shared the fewest per participant. The power of these second-hand stories was illustrated in comments by higher-level editors, who described how such narratives influenced their computer security behaviors at their organizations:

"Once you become aware of the possibility of ... a large-scale, wildly public hack, you become aware of how you use these systems differently." [E3]

Given how second-hand narratives can influence both the perception of security vulnerabilities and subsequent behaviors, managers in collaborative, networked organizations could benefit by leveraging storytelling as part of computer security training. Such trainings could take the form of encouraging employees to share accounts of their own experiences with others, or implementing an organizational mandate of community discussion around security breaches as a type of post-mortem exercise, similar to best practices in medicine after the loss of a patient. The principles of learning science as well as narratology hold promise for more robust training frameworks, and would benefit from further research.

References

[1] "Hackers compromise AP Twitter account." Associated Press. http://bigstory.ap.org/article/hackers-compromise- ap-twitter-account. April 23, 2013. Accessed October 15, 2016.

[2] N. Davinson and E. Sillence. "Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions." International Journal of Human-Computer Studies 72, 2 (2014), 154–168.

[3] A. Greenberg. "How The Syrian Electronic Army Hacked Us: a detailed timeline." Forbes. http://www. forbes. com/sites/andygreenberg/2014/02/20/how-the- syrian-electronic-army-hacked-us-a-detailed- timeline/¿, February 20, 2014. Accessed August 30th, 2016

[4] J. Henrichsen, M. Betz, and J. Lisosky. "Building Digital Safety for Journalism." United Nations Educational, Scientific and Cultural Organization. 2015.

[5] G. Klein, B. Moon, and R. Hoffman. "Making Sense of Sensemaking 1: Alternative Perspectives." IEEE intelligent systems 21, 4 (2006), 70–73.

[6] N. Mattise. "Syrian electronic army targets Reuters again but ad network provided the leak." ArsTechnica. http://arstechnica.com/security/2014/06/syrian-electronic-army-targets-reuters-again-but-ad-network-provided-the-leak/. June 22, 2014. Accessed September 25, 2016.

[7] N. Perlroth. "Hackers in China attacked The Times for last 4 months." http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0 . New York Times, January 30, 2013. Accessed October 16, 2016.

[8] N. Perlroth. "Washington Post joins list of news media hacked by the Chinese. http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html. The New York Times February 1, 2013. Accessed September 20, 2016.

[9] E. Rader, R. Wash, and B. Brooks. "Stories as informal lessons about security." In Proceedings of the Eighth Symposium on Usable Privacy and Security. ACM, 6. 2012.

[10] N. Sharma and G. Furnas. 2009. Artifact usefulness and usage in sensemaking handoffs. Proceedings of the American Society for Information Science and Technology 46, 1 (2009), 1–19.

[11] J. Wagstaff. "Journalists, media under attack from hackers: Google researchers." Reuters. http://www.reuters.com/article/us-media- cybercrime-idUSBREA2R0EU20140328. March 28, 2014. Accessed September 30, 2016.