People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap?

SUSAN SQUIRES
MOLLY SHADE
University of North Texas

Information Technology (IT) professionals are racing to keep up with cyber-security threats in the workplace. But, as any cyber-security expert will tell you, security technology is only as good as the people who use it. And, people are a mystery to most cyber-security professionals making them the weak link for security interventions in organizations. To broadly impact current cyber-security awareness, interventions and education, it is crucial to understand how security is understood and applied by the users of technology. Thus, it is no surprise that more and more cyber-security studies are focusing on the individual employee to understand computer-user risk mediation. However, users and their actions do not exist in a vacuum, and their perceptions and subsequent behaviors regarding security risk are shaped by a vast array of beliefs, social relations and workplace practices. This paper reports on a fresh theoretical approach to cyber-security as a group phenomenon that is well suited to ethnography. Results to date have demonstrated that communication between IT security professionals and users is not effective. Rather, this ethnographic study found that communication is breaking down between user communities and IT security departments because of mismatched understandings of the other. Each of the groups studied maintain myths and misconceptions about cyber-security that must be addressed and dispelled within their respective communities to secure the link between people and their technology.

INTRODUCTION

Cyber-security studies have traditionally focused on the i*ndividual* to understand computer-user risk mediation within work-based organizations using several very broad ways of conceptualizing how individual users confront risks. These are rational cost-benefit approaches, use of security metaphors, and usability design.

To frame our research and guide successful interventions in the workplace, the current research paradigm was expanded to bridge the knowledge gap between individual user studies and those that study groups using a theoretical approach that combines the work by Lave and Wenger on professional Communities of Practice (1991) with current security studies of users' mental models of risk perceptions. This conceptual framework situates *both* the user *and* Information Technology (IT) professional within the work context of each of their distinct work and professional communities, rather than using context as the stage for individual action, to gain insights on a community system level of users and the IT professional, which is needed to implement successful on-the-job security interventions. As both Codio (2012) and Bury et al. (2008) observed, security is practiced within a collective social context and they suggest that the goals and responsibilities shared by employees in the workplace shape individual security actions. Similarly Dourish and Anderson (2006) point out that individual risk perception is imbedded in a context of language, rhetoric, values,

2015 Ethnographic Praxis in Industry Conference Proceedings, pp. 47–57, ISSN 1559–8918.

norms, and cultures shared with other members of their work community or group. They argue that, while individual assessments of risk have value, results can still vary considerably depending greatly on the context, the shared values, the nature of information that must be protected, and the value placed on that information.

A Workplace Community of Practice can be identified by three structural characteristics: 1) shared education or knowledge provides common ground for members participation, guides learning and gives meaning to actions, 2) community creates the social fabric for learning and fosters interactions and a sharing of ideas, 3) practice provides group focus around which the community develops shares and maintains its core of knowledge (Wenger et. al. & 2002: 27 - 29). Using this model adds two key factors that differ from most previous research. First CoP focuses on shared beliefs and values of the group rather than individual motivations and perceptions. Secondly, CoP researchers have developed a set of well-defined tools for investigating the underlying mechanisms of socially shared practices and mental models are constructed and maintained by investigating 1) group norms and collaborative relationships, which bind the members of the community together as a social entity, 2) interaction that create a shared understanding of what binds them together, and 3) a set of 'shared repertoire' including work practices, language, and metaphors that is used in the pursuit of their joint enterprise (Wenger 1998:72–73). It is through the process of sharing information and experiences within the group that the members learn from each other (Lave and Wenger 1991). In the process, first as an apprentice and then as a full participant, each member internalize the group's mental models about how things work (Squires and Van De Vanter 2012). These processes are the objects of research for investigating CoP's mental models and provides a contextual structural system to study risk mental models, to understand risk mental model formation, and for bounding the work groups in which mental models are communicated and shared. It also provides an important frame for comparing the various work-groups within an organization including those of IT.

METHOD

Sampling

To pilot our theoretical model, three highly non-random Communities of Practice within a large educational organization were used to capture the shared beliefs and practices of each. The three groups were 1) security IT professionals, who were originally selected so as to compare "the experts" to the other CoPs, 2) business technology professionals who have knowledge of security risks but do not work in IT security, and 3) applied anthropologists. For IT three different work groups within one organization were interviewed and observed: a library help group, business services group and a group that supports public services. Participants were recruited using intercept, emailing and a snowball technique in which participants recommend co-workers as interview subjects. A total of 20 observation/interviews were conducted - 10 IT professionals, 4 business technology professionals and 6 anthropologists. Although the participant numbers were small, uncovering relevant shared patterns can be discerned with a relatively small number of people because of the non-random nature of each of the three populations (Handwerker and Wozniak 1997).

Data Gathering

To discover beliefs and practices of each of the three CoP memberships, an inductive approach, ethnography, was used. Ethnography is a holistic, systematic, and theoretically grounded approach to describe, interpret, and understand a group's belief and practices (Bernard 1998; Handwerker 2001; LeCompte & Schensul 2010; Squires and Byrne 2002; Weinberg 2002), which was originally developed to understand non-Western societies. In the last part of the 20th century ethnographic methodology was adopted by Western organizations because of its ability to reveal implicit underlying patterns within corporate groups (Crabtree et al 2000, Hughes et al 1994; Suchman 1995, Vinck 2003), and in technology sector studies (Franklin and Roberts 2006; Gusterson 1996; Knorr and Cetina 1999; Latour 1988; McNamara 2001; Rabinow 1997; Schatz 1991; Solomon 1997a, 1997b, 1997c; Star 1999). Ethnography is actually a set of methods for documenting 1) context by capturing physical and descriptive elements of the environment, 2) practices through written, photographic or video documentation of action, and 3) beliefs and values though semi-structured open-ended interviews that ask broad questions such as "Tell me about security" "Tell me a story about insecurity" "Show me how you stay secure" in a conversational style while ensuring that all topics on a structured interview guide are eventually addressed.

Analysis

Once interviews were transcribed, and field notes written, coding was used to identify a set of key security words, observations, and behaviors. Each code becomes a short phrase or statement. Two established methods for analysis were used: repetition and pattern matching. Repetition relies on "constant comparison" to search for similarities by making systematic comparisons across units of data (Ryan & Bernard, 2003:89). As Ryan and Bernard (2003:89) explain, "Repetition is one of the easiest ways to identify themes. Some of the most obvious themes in a corpus of data are those "topics that occur and reoccur" (Bogdan & Taylor 1975:83) or are "recurring regularities" (Guba 1978:53). Once coding was completed, patterns were sought using pattern matching, which is also called similarity and differences by Glaser and Strauss (1967:101–16). Theory provides the frame in which patterns in language, beliefs and practices are identified, described, and interpreted to allow similarities and differences to "emerge" creating a deductive "dataset" of shared beliefs and practices often indicated by shared rules and expectations. The next section describes the case studies that provide the data for the insights in this paper.

FINDINGS

From the group patterns, themes emerged that provided a structure for an integrated model of each of the three workgroups on the interrelationship of 1) beliefs, 2) group organization, 3) communication, and 4) subsequent behavioral patterns that impact cyber-threats and risk.

IT Community of Practice

The first community studied was IT services. Security IT professional CoPs have not been widely studied outside of large corporations and, for the most part, studies undertaken have

not been published. Yet, understanding why and how this group thinks about and implements security is key to understanding the organizational context of cyber-security.

Structure - The Director of the organization's IT services described IT as non-hierarchical and collaborative. This idealized description belied the reality in each of the IT departments, which were "a heavy hierarchal setup and chain of command" (IT team manager). Each of the three IT departments in the study are led by a single senior manager who is responsible for training, mentoring, counseling, and employee terminations. "He's the most important person on our staff. And without him as our linchpin, we are in big trouble" (IT team manager). This model is considered most appropriate for IT because each, "employee's job . . . has procedures for how we do certain things" (IT staff member). Within each department, there may be several highly coordinated work teams in which each employee has designated responsibilities and duties. Everyone is expected to 'work their way up' into more senior positions. One IT team manager described it as an apprenticeship model where members learn actively from more senior members. The purpose of the program is to develop their skills to advance to higher technical levels. At the beginning of their employment, each employee "picks a field and starts a kind of apprenticeship within different tracks such as Windows, Mac, Service, Management. They get two hours a week with a specialist to work with to develop the skills along the lines of the path they have chosen." By the time people graduate, there are several others in the "pipeline" ready to fill the position. As one IT team manager pointed out, this organizational model is effective because "they (IT staff member) know they will be able to grow, develop, and be rewarded."

Team members like working in this structure because the hierarchy provides a level of security that is important to ensure tasks are completed. As one senior IT manager commented, "I trust them to take care of things." While a junior staff member said, "If he (my boss) sends an email or leaves a sticky note, he trusts the team, to do it. The work balance is pretty equal and I've learned more and been able to take on more. When the two new people started, I played a part in teaching them the ropes. Sharing knowledge in general. That's kind of what we do."

Communication – There are difference between internal and external communication norms. Within the IT services top-down communication works well for most although a few bemoaned a lack of autonomy and transparency. Information is provided on a need-to-know basis so each tech can to do their job. Teams receive mandates from *above* and these mandates are then implemented through delegation to those *below* with work instructions relayed from senior to junior members. As work teams are in close physical proximity, communication is informal. When not face-to-face, team members use instant messaging or leave post-it-notes. If there are questions within the team or at the department level, each staff knows who to ask for assistance in the hierarchy. As one IT tech observed, "we have questions on a daily basis, so that open communication is important. ... I can ask them (supervisor) anything. And I usually do. This is the way we always did it."

While this communication style works well internally, it is less successful for external communication to the rest of the organizations. Only the Director of IT Services and IT department managers are responsible for information "coming from" and "going to" their group. IT staff rarely communicate with anyone outside of their team or department and "don't know what the other groups do."

External communication is more formal. As one senior IT manager noted, "I like sending people instructions by email because it's documented so you have something there which helps a lot, especially if I'm giving instructions to external people in the organization."

Security Beliefs – In this workplace context security is considered complex and difficult to communicate to junior IT staff much less others outside of IT. Junior members in the IT hierarchy insist they don't understand the complexities. Security becomes the sole responsibility of IT management. And, IT managers don't bother to communicate security threats anymore. The overall pattern suggests that IT managers think security is too technical for junior staff and, thus, far beyond the user. Instead IT managers put their time and energy into security technology "now that hardware and software are more secure" rather than communicating cyber security information to users. While security incidents are still treated with a high urgency, as one IT department manager commented, "perception of compromised incidents has changed from one of the sky is falling to one of it being more of a hassle." Educating the user is perceived as time consuming with dubious results. Users will have a breach sooner or later and there is not much IT can do. Security technology is the only real safeguard.

Summary – In this IT workplace community, security is considered too technical for users and communicating to them is not a priority. In fact it is considered non-productive. Users would be unlikely to follow orders even if they were instructed on how to protect themselves. Rather IT is focused on security technology as the primary strategy for protecting the organization from cyber threats. Users will continue to be a point of risk and it is up to them to protect themselves.

Business Technology Community of Practice – The second workplace community studied was a Business Technology department within a College of Business. The people in this department study and teach technology to business students. They are *very* literate in cyber security issues. Not surprisingly, everyone is aware of cyber security risk.

Structure – Business Technology is a department within the College of Business. There is a loose hierarchy based on the tenure system with ranks - full professor, associate professor, assistant professor and lecturer. There are also administrative staff who are at the bottom of the hierarchy. Members of this community may work together on a project, in committees or on other college business. Overall the members are pretty independent.

Security Communication – The members of this community actively keep their security knowledge up-to-date through professional listservs, conferences, and publications. They may also discuss security within their community but are less likely to interact with the IT group. Like the IT groups these technologically sophisticated business professionals shared IT's concerns that users, including their colleagues in other academic departments, are not sophisticated enough to understand security. The members of this community only feel comfortable talking about cyber security to their business technology colleagues assuming that other people would not have much to say on the subject.

Security Beliefs – There is universal faith in the IT security technology even though none interact with the security IT group. They all hold the belief that the security IT group will safeguard them "because it is pretty secure system." They also share IT's belief that users are the weak link in security. As one business professor noted, "Without adequate antivirus and computer literacy, users are most likely to get taken advantage of." All were in agreement that, "the objective of IT is to eliminate the human component."

Security Precautions – Security precautions were widely in use as "cyber security is important because we rely on technology so heavily, that to lose the data and capabilities that technology currently offers us would destroy all social norms as we know them today" (Business professor). They all echoed trust in IT and security technology and believe security will be maintained at work. Because of this shared belief none take any special precautions at the workplace. In contrast, security precautions for personal technology is important. Yet, all also admitted that there may be information on personal devices that is unprotected. For example one individual commented that she does worry that she keeps a copy of her son's birth certificate on her home computer while another does not have password for his personal phone. They also share the belief that the user is the weak link in security. But, unlike the IT community, this community was more pessimistic about security risk. "Everything can be hacked, and security precautions are merely strategies to minimize that risk. If you haven't been hacked, you will be" (Business Professor).

Summary – This technologically sophisticated group shared some overlapping beliefs with IT possibly because they are reading the same literature and attending similar conferences as those in IT services. These beliefs include a strong faith in workplace security technology and little faith in workplace users. They were much more pessimistic about security breaches especially regarding personal devices and information. Ironically personal security was exactly where they admitted taking risks.

Anthropology Community of Practice

The third community studied was a department of applied anthropology. While there was an expectation that this would be the least sophisticated of the three groups under study, sophistication levels were mixed. The range included a former computer scientist who considered himself technologically literate. At the other end was a self-proclaimed 'laissez-faire' cyber security risk taker.

Structure - This academic department is also loosely based on the tenure structure. However in this group most of the individuals operate as equals. While there is some cooperation around department activities, the individuals in this community act independently.

Security Communication - The individuals in this community are more likely to have extended conversations with other anthropologists outside of the workplace than within it. The topics of communication focus on areas of mutual research interest. Unless there is an academic interest in security, cyber-security is not discussed. None of the individuals in this

department have consistent communication with IT. Despite a lack of communication, they generally trust IT services and the security technology system in the workplace.

Security Beliefs - There were two important findings on perceptions of personal risk and the meaning of security. To begin, there was a lack of knowledge about what exactly cyber-security means. As one anthropologist noted "cyber security doesn't carry much meaning for me whereas 'internet security' seems more personal and relevant." Another said that she associates cyber security mostly with Edward Snowden and government-level surveillance rather than individual hackers. She noted that cyber security is a term with many definitions, and it's hard for her to really know what someone is talking about when they bring it up. More importantly was a shared belief that none of the members of this community are at risk because, as one lecturer explained, "no one is really interested in what I'm doing." This belief provided the rational for a lack of precaution. Another thought she was safe because she used Apple products sharing that "cyber security threats aren't as relevant to my devices." (Anthropology Professor). There was general consensus that the threat to their organizations was real but not to them at a work or personal level.

Security Precautions - Although uneven, the members of this community do take security actions based on what they read in the public domain or received in advise from IT friends. For example, most will proactively look for software updates, keep passwords and bookmarks secure, and change passwords when prompted. Although they feel they are taking the necessary precautions to protect their device, most reported that they have been hacked.

Summary - Two key findings are important in this community. First is the lack of knowledge about security terms: Cyber security and Internet security. The second is the belief that they are at low-risk for cyber security breaches because of one or more of the following: the information they possess isn't that useful or important, cyber-security is mostly a threat at the organization or state-level, and/or they are taking adequate precautions.

DISCUSSION

The Message

To date this investigation has revealed a communication breakdown between user workplace communities and IT services that is founded on fundamental-level mismatched understandings of the other that is perpetuated by the Communities of Practice, in which the various members belong. Within both IT and Business technical communities, security communication to workplace users is considered too complex to explain to a non-technical population or even junior IT members. The default position becomes one in which the IT community accepts that the user is the weak link in security but accepts that risk. For these two groups security technology is the priority.

Within the non-technical community of anthropologists, they struggled to avoid risk using whatever advice and instruction is in the public domain. Ironically it is not more technical information they need to aid them. There are two key areas that could be addressed. First, there is a fundamental need for users to understand the terms that IT

security professionals use. The current terms in use need to be demystified. Users need to understand that cyber-security is nothing more than the processes and practices used to protect devices and the networks they use. More importantly key misunderstanding and myths associated with cyber security need to be dispelled. For the user, crucial misconception can easily be corrected including:

- Cyber threats are directed at organizations not individuals
- Apple products are safe
- IT and their security technology will protect everyone

There are key myths that need to be dispelled within IT groups too including:

- Communications on security must be technical
- Users are the weak link that put the organization at risk
- Communicating to users is not productive

Messaging

There is also a mismatch between the organizational structures between IT workgroups and the wider organization that are maintained through definitional boundaries. Although most IT work groups see customer service as their goal, customers are also their key challenge. Communication *within* the IT communities is well established, but it is less effective once information is transferred *outside* of the group. Outside of IT both managers and staff find themselves unclear as to how to navigate the external "hierarchy" across disciplines which seems to contrast with their own structure. Nor do they understand the decision-making process of others, which is perceived to slowed things down and add bureaucratic complexity. The top down directives so effective within IT impede effective communication externally because they fail to provide contextual information on why an security action should be taken. External communication becomes compromised and both sides feel as if they are talking past each other and at different levels of expertise.

Messaging Methods

The method of communication is important too. For IT external and internal modes of communication use different tools and carry different meanings. While messaging and post-it notes are often used internally along with face-to-face interactions, emails are considered formal methods to document internal work and communicate to the outside. Formal communication internally and externally is linear where information is transferred from leadership to ground-level employees or from the "expert" to the wider organization. These methods do not work when external communication is attempted. The hierarchical model of communication reflects the internal one used by IT teams in which people are told only what they need to know along with instructions, and expected to comply. This messaging method is not effective to communities who are less hierarchical and with members who are less likely to follow direction without explanation.

CONCLUSION

Yes the weak link is people. More precisely the weak link is the beliefs, myths and misconceptions held by *both* IT and user workplace communities. If the weak link is people, cyber-security needs to be reconsidered at a more fundamental level by organizations such as the one studied. Effective cyber-threat interventions must begin by using a systemic, ethnographic approach to identify the perspectives and communication styles of both IT groups and that of the communities of users they serve. These must be identified and dispelled to reduce risk.

Susan Squires, Ph.D. is currently a professor in the Department of Anthropology at the University of N. Texas. Before joining UNT, she spent over twenty years in practice designing and conducting ethnographic research for a range of not-for-profit and private sector institutions. Her co-edited book *Creating Breakthrough Ideas (2002)*, documents her research theory and methodology.

Molly Shade holds an M.S. from the University of North Texas in Applied Anthropology. She is currently a User Experience Researcher for Hach, a water analyst company. She incorporates ethnographic and user-driven studies to inform product and service development for water technology.

REFERENCES CITED

Bernard, H. Russell, ed.
1998 *Handbook of Methods in Cultural Anthropology*. Altamira Press: Walnut Creek.

Bogdan, R., & Taylor, S. J.
1975 *Introduction to Qualitative Research Methods*. New York: John Wiley.

Bravo-Lillo, C., Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri
2011 Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy Magazine* 9(2): 18–26.

Bury, Sara, Johnathan Ishmael, Nicholas J. P. Race, and Paul Smith
2008 Towards an Understanding of Security Concerns Within Communities in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications* Pp. 478–483. IEEE.

Codio, Seey
2012 *Understanding Community Privacy through Focus Group Studies*. Master's Thesis, Department of Computer Science, Virginia Tech.

Crabtree, Andy, David M. Nichols, Jon O'Brien, Mark Rouncefield, and Michael B. Twidale
2000 Ethnomethodologically Informed Ethnography and Information System Design. *Journal of the American Society for Information Science*. 51(7):666-682.

Dourish, Paul, and Ken Anderson
2006 Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21(3): 319–342.

Dourish, Paul, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph
2004 Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing* 8(6): 391–401.

Franklin, S. and Roberts, C.
2006 *Born and Made: An Ethnography of Preimplantation Genetic Diagnosis* Princeton: Princeton University Press.

Glaser, B. G, & Strauss A.
1967 *Discovery of Grounded Theory. Strategies for Qualitative Research.* Sociology Press. New York: Aldine.

Gusterson, H.
1996 *Nuclear Rites: A Weapons Laboratory at the End of the Cold War,* Berkeley: University of California Press.

Handwerker, W. Penn, and Danielle F. Wozniak
1997 Sampling Strategies for the Collection of Cultural Data: An Extension of Boas's Answer to Galton's Problem1. *Current Anthropology* 38(5): 869–875.

Handwerker, W. Penn
2001 *Quick Ethnography.* AltaMira Press: Walnut Creek.

Hughes, John, Val King, Tom Rodden, and Hans Andersen
1994 Moving Out from the Control Room: Ethnography in System Design. *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work.* 429-439.

Knorr Cetina, K.
1999 *Epistemic Cultures: How the Sciences Make Knowledge*, Cambridge: Harvard University Press.

Latour, B.
1988 *Science in Action: How to Follow Scientists and Engineers through Society*, Cam- bridge: Harvard University Press.

Lave, Jean, and Etienne Wenger
1991 *Situated Learning: Legitimate Peripheral Participation.* Cambridge University Press.

LeCompte, Margaret D. and Jean J. Schensul
2010 Designing and Conducting Ethnographic Research: An Introduction in *Ethnographer's Toolkit*, Second Edition. AltaMira Press: Walnut Creek.

McNamara, Laura
2001 *Ways of Knowing About Weapons: The Cold War's End at the Los Alamos National Laboratory.* PhD dissertation, Department of Anthropology, University of New Mexico.

Möller, Sebastian, Noam Ben-Asher, Klaus-Peter Engelbrecht, Roman, Englert & Joachim Meyer
2011 *Modeling the Behavior of Users Who Are Confronted with Security Mechanisms.* Computers & Security 30(4): 242–256.

Rabinow, P.
1997 *Making PCR: A Story of Biotechnology,* Chicago: University of Chicago Press.

Ryan, G. W. & Bernard, H. R.
2003 Techniques to Identify Themes. *Field Methods* 15(1):85-109.

Schatz, Bruce R.
1991 Building an Electronic Community System. *Journal of Management Information Systems.* 8(3):87-107.

Solomon, P.
1997a Discovering Information Behavior in Sense Making: Time and Timing. *Journal of the American Society for Information Science.* 48(12):1097-1108.

1997b Discovering Information Behavior in Sense Making: The Social. *Journal of the American Society for Information Science.* 48(12):1109-1126.

1997c Discovering Information Behavior in Sense Making: The Person. *Journal of the American Society for Information Science*. 48(12):1127-1138.

Squires, Susan, and Michael L. Van De Vanter
2012 Communities of Practice in A Companion to Organizational Anthropology. D. Douglas Caulkins and Ann T. Jordan, eds. Pp. 289–310. John Wiley & Sons, Ltd.

Star, Susan Leigh
1999 The Ethnography of Infrastructure. *American Behavioral Scientist*. 43(3):377-391.

Suchman, Lucy
1995 Making Work Visible. *Communications of the ACM*. 38(9):56-64.

Vinck, Dominique, ed.
2003 *Everyday Engineering: An Ethnography of Design and Innovation*. Massachusetts Institute of Technology: Cambridge.

Wash, Rick
2010 Folk Models of Home Computer Security in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. New York, NY, USA: ACM.

Wash, Rick, and Emilee Rader
2011 Influencing Mental Models of Security: A Research Agenda in *Proceedings of the 2011 Workshop on New Security Paradigms Workshop* Pp. 57–66.

Weinberg, Darin, ed.
2002 *Qualitative Research Methods*. Blackwell Publishers: Malden.

Wenger, Etienne
1998 *Communities of Practice: Learning, Meaning, and Identity*. Cambridge University Press.

Wenger, E., R. McDermott, W. Snyder
2002 *Cultivating Communities of Practice: A Guide to Managing Knowledge.* Boston: Harvard Business School Press.

West, Ryan
2008 The Psychology of Security. *Communications of the ACM* 51(4): 34–4

EPIC *Advancing the Value of Ethnography*

epicpeople.org

EPIC promotes the use of ethnographic principles to create business value.

EPIC people work to ensure that innovation, strategies, processes and products address business opportunities that are anchored in what matters to people in their everyday lives. We draw on tools and resources from the social sciences and humanities as well as Design Thinking, Agile, Lean Start-up and other approaches to realize value for corporations from understanding people and their practices.

EPIC brings practitioners together as a community—at conferences and year-round on epicpeople.org—to create knowledge, share expertise, and expand opportunities. We are constantly learning and improving the ways that we achieve innovation and inform business strategy in a constantly changing world.

The annual EPIC conference brings together a dynamic community of practitioners and scholars concerned with how ethnographic thinking, methods and practices are used to transform design, business and innovation contexts. Attendees come from technology corporations, product and service companies, a range of consultancies, universities and design schools, government and NGOs, and research institutes. Submissions go through a double blind-peer review process and sessions are tightly curated. Final proceedings are published on epicpeople.org/intelligences with full-text search, as well as by Wiley Blackwell under ISSN 1559-8918.

Join us!

EPIC people learn from colleagues far and wide, at our workplace and elsewhere. We debate and push each other to improve, to experiment and to make change happen. There has never been a more important time for practicing ethnographers of all sorts to continue to have routine access to one another.

Your membership supports the first professional organization committed to the interests of anyone who seeks to advance the value of ethnography in business, research and nonprofit settings. Over the last year, memberships have supported crucial new resources to advance the professional interests of our community, including critical content, a job board and a business directory. EPIC is a 501(c)(3) incorporated in the state of Oregon.

epicpeople.org/membership

Board of Directors