IEEE Security & Privacy, Volume: 14, Issue: 3, May-June 2016, pp82 - 87
DOI: 10.1109/MSP.2016.57

Editors: Angela Sasse, a.sasse@cs.ucl.ac.uk | Alessandro Acquisti, acquisti@andrew.cmu.edu

In Our Orbit

Security Dialogues:

Building Better Relationships Between Security and Business

Debi Ashenden and Darren Lawrence | Cranfield University at the Defence Academy of the United Kingdom

A policeman sees a drunk man searching for something under a streetlight and asks what he's lost. The drunk man says that he's lost his keys. They both look under the streetlight together. After a few minutes, the policeman asks the man whether he's sure he lost them here; the drunk replies "no," and that he lost them in the park. The policeman asks why he's searching here, and the drunk replies, "This is where the light is."

The "streetlight effect"[1]—originally less flatteringly referred to as the "drunkard's search"[2]—is a form of observational bias. It recognizes our tendency to look for solutions to problems where it's easiest to find them, such as under a streetlight. In this article, we describe what happened when we set out to deliberately move away from the "streetlight" of traditional approaches to cybersecurity and look more broadly at where solutions might lie. We applied a technique called *security dialogues* to improve the conversation between security practitioners and organizational staff. We hoped that, if successful, we might also improve security processes and contribute to the development of a stronger security culture.

Social Practice of Security

Security dialogues describe the two-way communication between security practitioners and staff. These dialogues are part of the rituals, routines, stories, and symbols that together form organizational culture.[3] To change organizational culture, security practitioners need soft skills—those interpersonal or "people" skills that encourage effective communication and collaboration.[4]

The UK's Centre for the Protection of the National Infrastructure (CPNI) has performed significant research on security culture within organizations. One such study concluded that poor security culture and poor communication among business areas hampered risk management, particularly insider threats.[5] Other research has shown that chief information security officers often struggle to communicate persuasively with staff because they lack soft skills, a problem that's further exacerbated by their failure to take a "participative approach" to solving security problems.[6]

These issues are particularly relevant to risk assessment. Security practitioners and staff usually start their discussions around the topic of risk; however, cybersecurity risk assessment methodologies treat the organization in which they are implemented as knowable and unproblematic. Despite Richard Baskerville's warning that risk analysis that depends on weak statistical models built in to make risk calculations appear robust are "voodoo economics,"[7] the cybersecurity community still pays more attention to the mechanics of the risk assessment process, underexploiting the value of risk management as a communication tool. A meaningful risk assessment needs good quality information and must yield a final report that's persuasive enough for the business to act upon it. Thus, information gathering and risk communication are part of cybersecurity risk assessment, and security practitioners must be able to engage in productive dialogues to succeed in these activities.

In the real world, there's often a shortfall between the mandated, formal security processes in an organization, and what actually happens: projects have to finish, systems have to run, and the business has to move forward. The social practice of security[8] flourishes in the compromises and gaps between the processes that seek to shepherd the activities and outputs of security enactment.[9] It's here that we see an opportunity to improve the security dialogue, risk communication, and security culture.

Aiming for Concordance

The organization we worked with was seeking to develop “constructive interactions between security and the business in a way that both sides value and which holistically benefits the business.”

We performed an initial set of six scoping interviews, through which we discovered that poor interactions between cybersecurity practitioners and staff often resulted in a lack of trust on both sides. Without trust, staff failed to engage with security issues or even actively avoided it. Thus, cybersecurity was either ignored or given insufficient time and resources in projects. Software developers were particularly wary of revealing innovative solutions to security practitioners for fear of being shouted down, which one interviewee referred to as “shooting the baby.” Developers felt that security practitioners were judging them and that the security process was simply another hurdle to overcome.

Staff told us that they wanted security practitioners “to be seen as people like us, and fighting for the same side.” Unsurprisingly, when this wasn’t perceived to be the case, one or both sides were reluctant to engage in dialogue. The knock-on effect of this was that security practitioners didn’t fully comprehend the risks posed by business practices or new systems. They only had a partial view because they only asked the specific questions needed to meet the formal requirements of the organization’s security processes. Staff, on the other hand, only provided the information specifically requested and didn’t reveal other potentially relevant information about risks.

Where good relationships existed in the organization, there was trust and open communication. For example, there were a few cases “where a growing level of trust has allowed some areas to get some things off their chests and fess up to some stuff which we ought to have been told about, but Nobody Got Round To Telling Security” [capitals in the original].

Our aim was to help security practitioners develop a relationship in which staff would share this type of information freely. We took inspiration from research into doctor–patient interactions. This, too, is a relationship where solutions to problems rely on constructive dialogues. Expertise must be communicated in a way that builds trust, which, in turn, can lead patients to change their behavior. Studies have shown that regardless of the amount of time doctors spend discussing, assessing, and making recommendations, half of patients fail to carry out their treatments as recommended. In fact, between 10 and 25 percent of hospital admissions can be traced to non-adherence to doctors’ recommendations—and that this is just as likely to happen with organ transplant patients as with those with more minor ailments.[10] Researchers are trying to find a way for doctors and patients to reach concordance—a “mutual understanding and agreement”[10]—such that they can co-design a treatment plan. If doctors and patients both participate in the treatment plan’s design, patients are much more likely to stick to it. We recast what we learned about the doctor–patient relationship onto the security practitioner–staff relationship to understand the journey that we needed to take to improve security dialogues.

Security Dialogue Workshops

We designed a range of activities to help security practitioners understand why staff act the way that they do. We incorporated research from the medical world, as well as theories of exchange and influence from social marketing.[11] We applied techniques for designing interventions that would encourage behavior change,[12] and questioning and conflict-resolution skills developed from counseling. We wanted to give participants a broad base of tools and techniques to try, and then refine and adjust this initial selection over time.

After packaging the activities into a workshop, we conducted three pilot workshops, each lasting three days with 18 participants in total. The workshop introduced ideas for discussion before locating them in general examples and then applying them to a realistic cybersecurity scenario. When, in the first pilot workshop we moved straight into the security scenario, participants requested more general examples first. We adjusted accordingly, and ultimately received such feedback as “It was very useful to carry out the exercises based on different scenarios.”

The authors were part of a team of three researchers that ran the workshops. This number meant that over the course of the workshops, one researcher was always dedicated to the task of taking field notes. We also collected participant outputs: completed tables from the exercises, idea flip charts, design sketches from experiential exercises, and so on. In the final iteration of the workshop, we also collected schematics showing the participants’ perceptions of where power was located in the security process. Finally, we collected daily feedback sheets from each participant.

Workshop Sessions

One topic that we discussed with workshop participants was whether they thought it was possible for both security practitioners and staff to feel satisfied with the security process—or whether for one party to be satisfied, the other had to feel that they’d lost? In other words, did they think that security was a zero-sum game, or did they see the possibility of a win–win outcome? Reassuringly, the overwhelming response was that it could be win–win, although some factors got in the way. First, security and the security practitioner’s role came with baggage that was difficult to overcome. Many staff and security practitioners had had negative experiences with previous projects. Security practitioners felt that they were constantly “firefighting” in the face of other parts of the organization. During the scoping interviews, one staff member commented that security practitioners “are like a rock in a stream, we just flow round you.” One security practitioner pointed out that “there are few projects where project managers get done for lack of security.” Second, there was the problem of the security process being perceived as nothing more than a “paperwork, procedural, activity.”

An initial workshop session explored the benefits and downsides for staff of engaging early with security. We sought to uncover why project teams often delay engagement with security practitioners. Participants, when asked to put themselves in the place of project teams, found it easy to see the benefits of not engaging early: staff felt that projects progressed “quicker,” with “less hassle,” which in turn meant “lower cost.” It also meant that they wouldn’t “get an answer they [didn’t] want” and that they could “claim ignorance” of security requirements. The project could still be approved “due to political considerations,” particularly if there was a business need. The perceived benefit of delay was that it was “easier to seek forgiveness than permission.”

The barriers to early staff engagement included departmental processes and contractual requirements but also “management” that didn’t prioritize security. Previous “bad experiences” with the security process were cited as another barrier, as were “fear of failure” and “lack of resource.” As the participants highlighted, there’s no point to the security practitioner engaging early if the “culture is to deliver at all costs.” A small number of participants concluded that some issues stemmed from the fact that they themselves were “not able to articulate the risks we are taking.”

We recognized early on that it was difficult to measure “a good relationship between security and the business.” In one session, we discussed how to operationally define a concept so that it’s measurable; we started with the example of how one might measure a hidden quality like thirst. We demonstrated how to look for behavioral dimensions or properties that could then be categorized into observable and measurable elements (for example, with thirst, one element could be the amount that people were observed drinking). Participants applied these ideas to the concept of the relationship between security and the business. They developed measures that would indicate whether there was a good, trusting relationship between security practitioners and end users, including

- the number of emails that were exchanged with security,
- the tone of emails,
- how early on security practitioners became engaged in the project, and
- the number of security features that had to be retrofitted into a process or system.

We ran a double session on questioning skills and conflict negotiation to allow participants to experiment with basic questioning skills and techniques, and see how they might be applied in a professional context when differences of opinion occurred. The approach underpinning these sessions came from counseling. Participants tackled concepts such as neutrality, positivity, and curiosity by using open, contrast, and distance question styles.

The questioning-skills session proved the most difficult for participants. For security practitioners, the focus is on "technical training," which participants believed was easier to do than exploring the "soft" aspects of the security problem.

They were concerned that asking soft or open questions would be seen as unprofessional. They felt that other end users would "just want the professional approach." As a consequence, they wanted to know how to make the questions "soft enough and still feel value in the job we do." This suggests that the practitioners were more concerned with how they were perceived than with doing something that staff wouldn't like. As one participant explained, "we aren't experts and might come across as strange." They found it difficult to see how they could mix hard and soft, open and closed questions. One delegate said, "I don't get how this will answer the fundamental questions we need to know." They thought it "would be difficult [to] think of questions" and, indeed, they did find this difficult during the workshops. They felt they would need to "study for years to get good," and there was a general perception that although it "makes sense," the approach would be "very difficult." Participants said it was both "easier to ask hard questions" and also "quicker."

From the first workshop we learned that we needed to slow the pace of material delivery. We were told that there was "a lot of information to consider in one go," and some participants requested a longer, one-week workshop. Mindful of costs and resourcing, we refined the workshop content rather than extending its length. In the first workshop, we were told that the exercises we had devised were "too theoretical" and that we needed more "practical demonstration." Our intention had been to use role-play to practice the questioning techniques, but participants were reluctant. We succeeded when we stripped the questioning-skills session back to the basics and used a facilitated role-play between two of the researchers, with the workshop participants devising the questions. One participant said, "I used to think it's about getting my questions answered—today I've changed my mind with things as I do need to influence."

Participants said that they would try to develop a broader range of dialogues by mixing hard and soft questions and "applying the different interviewing techniques to difficult discussions." They thought it was "good to learn alternative ways to pose questions … particularly the soft techniques." Alongside broadening the type of questions that they would ask, they also said that they intended to "consider the manner/language/tone, etc. when asking questions" and would "pause—allow more time for reflection." Finally, they believed that they would use the "techniques learned today during more heated discussions." They recognized that doing so would "limit unnecessary escalations and emotions taking control."

The behavioral change session gave participants the opportunity to consider some easy approaches to influence staff behaviors. The session built on social marketing research that uses the concepts of "hug, smack, shove, and nudge" to develop a range of approaches to achieving behavior change in a soft problem space.[13] Participants recognized that they'd previously relied heavily on using a smack, and came to realize the benefits to be gained by more hugging, that is, giving positive feedback to encourage good behavior. One participant commented, "Hug, smack, shove, nudge. Good exercise which I found hard work—but could see what it was trying to achieve."

The issue of power arose numerous times in the first two workshops. In the final workshop, we asked participants to consider the issue of power over the life cycle of a project. We wanted to know whether they felt that their power was equal throughout the project, or whether either they or other staff held greater power at certain times. We also asked them to consider the kind of power they thought they had: was it power as an individual, power that came as a result of their security practitioner role, power from being able to persuade or influence, or power that came from being able to offer rewards?

This task raised conflicting views. Participants were split over whether their power increased just before the system was due to go live. About half thought that their power increased at this point because staff needed something from them: "if they need help at the last minute, they become more pliant." Through the rest of the project life cycle, security practitioners believed that they had less formal power than other staff. Any power they had varied over time and depended on whether they had the skills to influence or persuade staff to do what they required. They pointed out that their power decreased when potential penalties weren't enforced.

Finally, we conducted a "scrapheap challenge": an experiential session in which participants engaged in a participatory approach to developing a security solution, and experienced the satisfaction (or failure) of a negotiated solution. The task was to design a system using everyday security techniques but without using standard technical solutions. Each group had to design and agree upon a solution, showcase their design to the other groups, and then choose the best solution.

After three pilots, the prototype workshop is now stable, and we're getting positive participant feedback, such as "the exercises were definitely thought provoking." When asked what should be changed about the workshops, we're being told, "more of the same" and "all useful—no change." But we'll need to be flexible: the security practitioner role varies from one organization to another, not least depending on whether the security practitioner is an employee in the organization, or a contractor or consultant.

Impact on Security Practitioners

Our participants gained a better appreciation of their effect on the wider organizational context. One said, "[We] play a greater role in interfacing between an unsatisfactory mandated process and the 'operational' business than I realized." Another said that they would "think about the inclusion of how we are thought about by the business, in terms of success and satisfaction." One participant highlighted the value of other security practitioners learning the soft skills covered in the workshops: "This sort of training is not available, as soft skills courses are being overlooked." The specific activities participants said they would do differently as a result of the workshops included building better engagement with project stakeholders, developing a more constructive dialogue, and using a range of techniques to encourage better behaviors. They said they would "try and understand … the developer's point of view" and remember that "some people are personally vested in a system and take criticism to heart." This was summarized in the feedback as "learning to see both sides of the argument" and taking "more consideration of other's views in a project."

We developed an intervention that addresses the security dialogues that occur in the space between and around formal organizational security processes. It's through these dialogues that security practitioners can make up the shortfall between the security process and the real-world context in which it operates. Our aim in improving security dialogues is to influence the social practice of security and encourage a virtuous circle of positive engagement. The dialogues themselves help ensure that the process fits its purpose and is effective and satisfying to all parties involved. In turn, this provides better inputs and outputs for risk assessment and is more likely to strengthen the security culture.

By using a strong participative approach, the workshops generated a rich set of data, some of which is being used in a study to further develop measures of satisfaction in the relationship between security practitioners and staff. The positive evaluation ratings we received demonstrated that participants found the workshops interesting and useful and, more importantly, that they'd encourage others to attend. Finally, we learned that when a security process works well, it's often because the security practitioner has good soft skills.

Acknowledgments

This work was partially funded by the Government Communications Headquarters and the Centre for Research and Evidence on Security Threats (ESRC award ES/N009614/1).

References

1. D.H. Freedman, "Why Scientific Studies Are So Often Wrong: The Streetlight effect," *Discover Magazine*, 2010, p. 26.
2. A. Kaplan, *The Conduct of Inquiry: Methodology for Behavioral Science*, Chandler, 1964.
3. G. Johnson, K. Scholes, and R. Whittington, *Exploring Corporate Strategy: Text and Cases*, Pearson Education, 2008.
4. D. Ashenden, "Information Security Management: A Human Challenge?," *Information Security Technical Report*, vol. 13, no. 4, 2008, pp. 195–201.
5. "Insider Data Collection Study: Report of Main Findings," Centre for the Protection of the National Infrastructure, 2013; www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf.
6. D. Ashenden and A. Sasse, "CISOs and Organizational Culture: Their Own Worst Enemy?," *Computers & Security*, vol. 39, 2013, pp. 396–405.
7. R. Baskerville, "Investigating Information Systems with Action Research," *Comm. Assoc. Information Systems*, vol. 2, 1999, pp. 1–32.
8. A. Reckwitz, "Toward a Theory of Social Practices: A Development in Culturalist Theorizing," European J. Social Theory, vol. 5, no. 2, 2002, pp. 243–263.
9. I. Kirlappos, S. Parkin, and M.A. Sasse, "'Shadow security' As a Tool for the Learning Organization," ACM SIGCAS Computers and Society, vol. 45, no. 1, 2015, pp. 29–37.
10. L. Myers and C. Abrahams, "Beyond 'doctor's orders'," The Psychologist, vol. 10, no. 11, 2005, pp. 680–683.
11. D. Ashenden and D. Lawrence, "Can We Sell Security Like Soap?: A New Approach to Behavior Change," *Proc. Workshop on New Security Paradigms* (NSWP 13), 2013, pp. 87–94.
12. J. French, R. Merrit, and L. Reynolds, *Social Marketing Casebook*, Sage, 2011.
13. J. French, "Why Nudging Is Not Enough," *J. Social Marketing*, vol. 1, no. 2, 2011, pp. 154–162.

Debi Ashenden is a Reader in Cyber Security and Head of the Centre for Cyber Security & Information Systems at Cranfield University at the Defence Academy of the United Kingdom. Contact her at d.m.ashenden@cranfield.ac.uk.

Darren Lawrence is a Senior Lecturer in Behavioral Science at Cranfield University at the Defence Academy of the United Kingdom. Contact him at d.lawrence@cranfield.ac.uk.

Security dialogues: building better relationships between security and business

Ashenden, Debi

2016-08-09

Ashenden D, Lawrence D. Security dialogues: building better relationships between security and business. IEEE Security and Privacy Magazine, Volume 14, Issue 3, 2016, pp. 82-87
https://doi.org/10.1109/MSP.2016.57