A Fragmented Whole: Cooperation and Learning in the Practice of Information Security

Ashwin J. Mathew
Packet Clearing House
ashwin@pch.net

Coye Cheshire
UC Berkeley School of Information
coye@berkeley.edu

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

PCH
Packet Clearing House

Published February 2018

Summary

Of the many problems faced by the field of information security, two are particularly pressing: cooperation and learning. To effectively respond to threats and vulnerabilities, information security practitioners must cooperate to securely share sensitive information and coordinate responses across organizational and territorial boundaries. Yet there are insufficient numbers of personnel who have learned the competencies necessary to build information security teams.

Current policy responses to these issues treat cooperation and learning as independent problems to be dealt with through *institutional arrangements*. In this view, cooperation may be enabled by industry associations or government agencies that act as hubs for coordination and information sharing; and learning may be addressed by appropriate degree and certification programs. In contrast, we argue that cooperation and learning in information security are fundamentally connected problems which must be addressed together.

Through ethnographic and survey research, we found that information security relies to a significant degree upon *interpersonal trust relationships* - rather than only institutional arrangements - for both cooperation and learning. The more sensitive the information to be shared (as is typically the case with novel threats and vulnerabilities), the more likely it is that cooperation will take place within tightly bounded trust circles, in which participants know and trust each other. Learning the more sophisticated competencies of information security relies upon access to these bounded social contexts, in which skills and knowledge circulate securely. In order to cooperate effectively and engage in more sophisticated learning, information security practitioners must build their connections to the interpersonal trust relationships that structure the field of information security. Our research indicates that institutional arrangements can provide the foundations for interpersonal trust relationships, but cannot substitute for them; just as interpersonal trust relationships cannot substitute for the functions that institutional arrangements offer.

Information security is a *fragmented whole*, composed of strongly bounded, sparsely connected trust groups and organizations that seek to ensure the trustworthiness of participants. We suggest a substantially different set of policy interventions to support cooperation and learning in information security, focusing upon building interpersonal trust relationships, as much as on building institutional arrangements. Our recommendations include suggestions for stronger information sharing communities, for building relationships between educational institutions and information security practitioners, and for supporting diversity.

Contents

About the Authors

Ashwin J. Mathew is a researcher at Packet Clearing House. He is also a Visiting Scholar at the UC Berkeley School of Information, a Fellow at the Slow Science Institute, and an affiliate of the UC Berkeley Center for Long-Term Cybersecurity. He studies Internet governance through a focus on the relationships, practices, and institutions of the technical personnel who operate Internet infrastructure. He holds Ph.D. and Master's degrees from the UC Berkeley School of Information. Prior to his doctoral work, he spent a decade working as a software engineer and technical architect in companies such as Adobe Systems and Sun Microsystems.

Coye Cheshire is an associate professor at the UC Berkeley School of Information and an affiliate of the UC Berkeley Center for Long-Term Cybersecurity. His work focuses on how various forms of exchange are produced and maintained on the Internet and, more broadly, in computer-mediated exchanges. His current research topics include the role of trust and cooperation in interpersonal online interactions, collective behavior and online collaboration, and social incentives and motivations to contribute in online environments.

About the Center for Long-Term Cybersecurity

With a generous starting grant from the Hewlett Foundation, the Center for Long-Term Cybersecurity (CLTC) was established in 2015 as a research and collaboration hub at the University of California, Berkeley. Housed in the School of Information, the Center creates an effective dialogue among industry, academia, policy, and practitioners, with an aim to foster research programs, technologies, and recommendations. CLTC's work is founded on a future-oriented conceptualization of cybersecurity – what it could imply and mean for human beings, machines, and the societies that will depend on both.

For more information, see https://cltc.berkeley.edu/.

About Packet Clearing House

Packet Clearing House is the international organization responsible for providing operational support and security to critical Internet infrastructure, including Internet exchange points and the core of the domain name system.

For more information, see https://www.pch.net/.

Acknowledgments

We would like to thank all the information security practitioners who graciously gave of their time and insight for our research. This report would not have been possible without all those who responded to our naivety with good humor in interviews, and those who took the trouble to answer a somewhat lengthy and complex survey. We hope that we have done justice to their experiences in the field of information security. We particularly thank the Information Systems Security Association and Women in Security and Privacy for the invaluable support they provided for our research.

We are grateful to the Center for Long-Term Cybersecurity at the University of California, Berkeley, which provided the grant funding for this research. We also thank Packet Clearing House for additional material and logistical support for our work.

The intellectual foundations for this report were laid in many places, but a few deserve particular acknowledgement. One of the authors (Ashwin J. Mathew) was provided a fellowship that supported the writing of this report, by Professor Jean Lave at the Slow Science Institute. Initial results from our research were presented at the inaugural Ostrom Workshop Colloquium on Cybersecurity and Internet Governance at the University of Indiana, Bloomington, which was organized by Professor Scott Shackelford, with a discussion led by Professor Barbara Cherry. Dr. Suzanne Thomas of Intel Research offered a generous and insightful critique of an early paper reporting on our research. Our thanks go to these scholars, the fellows at the Slow Science Institute, and the participants at the Ostrom Workshop Colloquium for lively conversations from which this report benefited immeasurably.

1 Introduction

The field of information security is at a challenging moment. It often seems that each new day brings with it a fresh set of vulnerabilities and attacks, calling for better information sharing and cooperation to manage effective collective responses across organizational and territorial boundaries. At the same time, it remains difficult to build the information security teams required to mount these responses, for there appear to be insufficient numbers of trained information security professionals to staff these teams. At first glance, the problems of cooperation and education seem unrelated; in fact, current cybersecurity policies treat them as independent problems. In contrast, our research indicates that cooperation and education (or learning) in information security are intimately connected problems that must be addressed in concert.

We refer to learning – instead of education – to highlight the importance of the skills and knowledge of information security learned in the practice of *doing* information security, in comparison to those obtained in formalized institutional educational settings (e.g., certificate and degree programs). We make a similar distinction in analyzing cooperation for information sharing, by contrasting sectoral and government-led institutional information sharing arrangements with more constrained, tightly knit interpersonal information sharing arrangements leveraged in the everyday practice of information security.

Our research juxtaposes *interpersonal relationships built on social trust* with *institutional arrangements* for cooperation and learning in information security. By focusing on interpersonal relationships alongside institutional arrangements, we draw attention to the social connections leveraged by information security practitioners in their everyday practice for cooperation and learning. Analyses of institutional arrangements for these purposes focus on inter-organizational relationships, and the legal regimes which enable such relationships. In contrast, interpersonal relationships depend upon social trust formed as information security practitioners come to know one another in the process of working together, and demonstrate their competence and trustworthiness in handling sensitive and confidential information.[1]

> *"Our research juxtaposes interpersonal relationships built on social trust with institutional arrangements for cooperation and learning"*

It could be argued that the reliance upon interpersonal trust relationships is merely an artifact of an early stage of development, and that, as the field of information

[1] See Appendix A for a review of the literature through which we analyze trust, cooperation, and learning.

security evolves, institutional arrangements will provide long-term solutions to the problems we raise. However, our research indicates that interpersonal trust relationships will likely always play a critical role in cooperation and learning among information security practitioners, due to the interactions between three key characteristics which we believe define the field of information security:

1. **Confidentiality**: The primary function of information security is to secure sensitive information within organizational – and sometimes territorial – boundaries. Information to be protected includes proprietary information, and information subject to protection under government regulations (e.g., medical records, or personally identifiable information), but also operational information required for information security, such as information about emerging vulnerabilities and ongoing attacks.

2. **Interdependence**: The need for confidentiality is contradicted by a parallel need for interdependence. Sensitive information must often be securely shared between different organizations and transmitted over, or stored on, third-party systems. Information about attacks and vulnerabilities needs to be securely shared between information security professionals in different organizations and potentially in different countries. This contradiction lies at the heart of information security: secure information relies on shared information.

3. **Novelty**: By its very nature, information security is premised upon the management of novel exceptional conditions. Once an attack or vulnerability has been analyzed, the task of information security is to maintain effective mechanisms for remediation. However, every new attack or vulnerability requires an original analysis, and thus new mechanisms for remediation.

It is essential to study the interactions among these three characteristics in detail, as they represent problems that will always be part of the field of information security. We study institutional arrangements and interpersonal trust relationships for cooperation and learning though these characteristics by examining the following research questions:

1. **How is the contradiction between confidentiality and interdependence resolved to enable cooperation for information security?** Information security practitioners must balance these two requirements in order to effective in their practice, as secure information relies upon securely shared information.

2. **How is the contradiction between confidentiality and novelty resolved to enable learning for information security practitioners?** As with many fields, learning is an ongoing process in information security, as practitioners constantly acquire new skills and knowledge as they work to uncover and respond to novel attacks and vulnerabilities. However, in order to address novel problems securely, information about them cannot be shared openly.

> Information security practitioners must be able to access confidential information about novel problems in order to continue to learn and develop the knowledge and skills of the field of information security.

Throughout the research presented in this report, we examine these two questions by contrasting the functions of institutional and interpersonal mechanisms in resolving the contradictions that we raise. Institutional arrangements such as national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), and industry-led Information Sharing and Analysis Centers (ISACs) play a critical role in enabling inter-organizational and cross-territorial cooperation for information security. However, interpersonal relationships play a similar role in enabling cooperation within restricted trust groups to which access is granted by individual – rather than organizational – reputation.

Similarly, institutional mechanisms for learning in information security – such as certificate and degree programs – are essential for training and credentialing information security practitioners for entry to the job market. Yet learning in information security is not constrained only to these institutional environments, as practitioners continue to learn and develop new skills and knowledge in dealing with novel exceptional conditions which they experience in their practice. However, these experiences are bounded by confidentiality within organizational contexts and by restricted groups and institutional mechanisms that enable confidentiality in interdependent systems and relationships, across organizational and territorial boundaries. As a result, the skills and knowledge of information security are maintained through ongoing processes of learning that take place within bounded, secure contexts. The drive to secure information ensures that these skills and knowledge are limited to circulation within trustworthy social contexts and cannot easily be extracted into institutionalized degree and certificate programs.

> *"Information security is a fragmented whole, constituted by sparsely connected, mostly closed circuits of knowledge"*

As a field, information security is a fragmented whole, constituted by sparsely connected, mostly closed circuits of knowledge. There is no single information security community but rather a plethora of constrained and only partially overlapping information security communities. Some of these are more permanent, meant to foster ongoing cooperation; others are transient, focused on addressing a particular attack or vulnerability. These communities vary from those named and recognized by all involved to others that are simply small circles of trustworthy acquaintances. Each has its own distinct norms and pathways to admission. It is sometimes necessary – but rarely sufficient – to gain access to these communities by virtue of organizational affiliation. In consequence, a central challenge information security practitioners face as they grow in their careers is that of building the interpersonal relationships that will help them become aware of, and gain access to, these communities.

The conventional figure of the information security practitioner is either that of the *hacker* – the brilliant individual who is born with inherent capabilities – or the *engineer* – the individual whose capabilities come through training. Our story is that of a third kind of figure, the *cooperator*, who learns and engages in the practice of information security through the process of building interpersonal trust relationships for ongoing cooperation.

Our research indicates that the risks and contradictions inherent in three key features of information security – confidentiality, interdependence, and novelty – will always require interpersonal relationships, based upon social trust. Institutional mechanisms can provide necessary supports for these relationships but cannot substitute for them. Interpersonal trust relationships provide the necessary social glue to build a whole from the fragmented social contexts that constitute the field of information security.

A focus on the configurations of combined interpersonal relationships and institutional arrangements required for effective cooperation and learning in information security calls for substantively different interventions than current policy responses which center institutional arrangements. Institutional responses offer the advantage of clearly separating concerns: institutions for cooperation may be developed independently of institutions for learning the skills of information security. In contrast, a view of information security through the lens of interpersonal relationships illustrates how cooperation and learning occur together as part of the same social processes that unfold in the practice of doing information security.

We begin by presenting our research methods, and quantitative and qualitative data in the "Data and Methods" section. In the section "Cooperation and Trust" we detail the ways in which the practice of information security is fundamentally cooperative and reliant upon interpersonal trust relationships. We build on this understanding in the following section, "Education and Learning in Practice", to show how and why the processes of learning the skills of information security proceed in large part in the practice of doing information security. In "Building Trust" we explore the challenges of building and maintaining trust relationships. The structuring of the field of information security by interpersonal trust relationships has important implications for issues of diversity, which lie at the intersection of gender, race, class, and other markers of identity. We remark upon these implications in "A Homogeneous Field". Finally, we offer ideas for supporting the continued development of the field of information security in our "Conclusion and Recommendations".

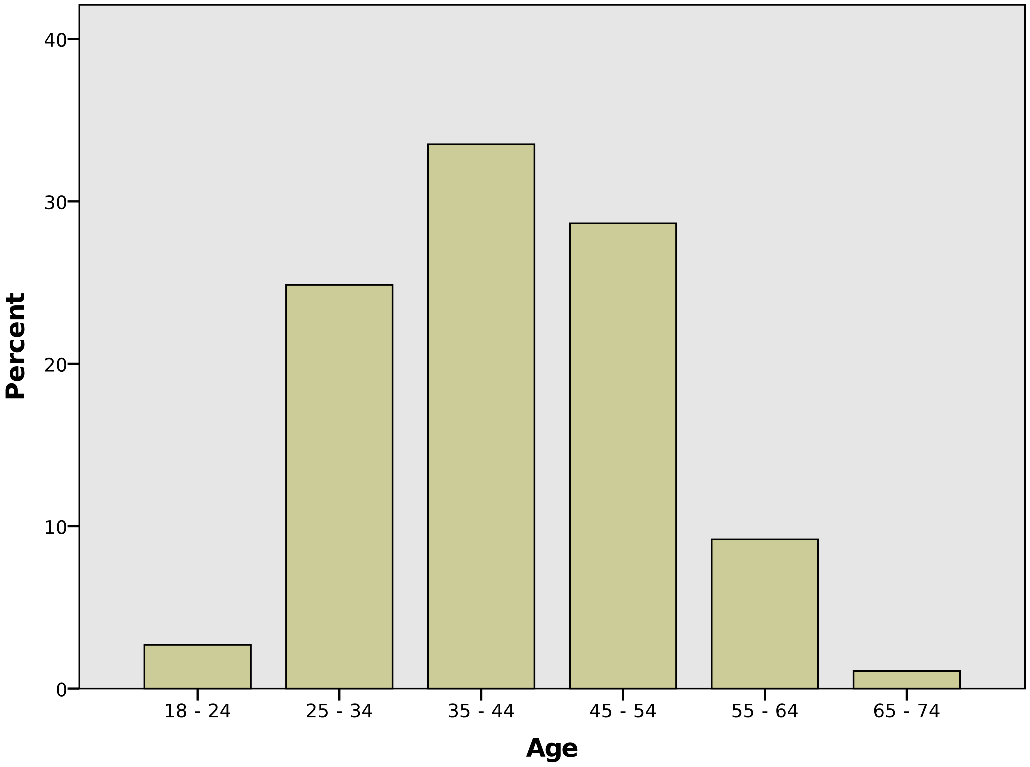
2 Data and Methods

We employed a mix of qualitative and quantitative methods for this research, including interviews with information security practitioners, participant observation at information security conferences, and a survey of information security practitioners.

We conducted participant observation at three information security conferences, each of which represented a distinctive slice of the information security world. First, we attended a meeting of the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) in February 2016 in San Francisco, USA. M3AAWG is an international industry association which, as the name suggests, is dedicated to combating issues such as spam and malware in online messaging channels, especially email. M3AAWG meetings are restricted to M3AAWG members and their guests. We obtained an invitation to attend the M3AAWG meeting through our affiliation with Packet Clearing House. Next, we attended a meeting of the Forum for Incident Response and Security Teams (FIRST) in June 2016 in Seoul, South Korea. FIRST is an international organization that brings together government and private sector groups that function as coordination points to respond to information security threats and vulnerabilities. These groups are generally termed Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). Finally, we attended the Security BSides conference in San Francisco in February 2017. Security BSides are local, community-run conferences held in cities around the world. The participants at Security BSides tend to be information security practitioners of a variety of experience levels from local information security communities, in contrast to the relatively more senior practitioners who travel to attend M3AAWG and FIRST meetings wherever they may occur. Observations from these conferences were captured in field notes for analysis.

Our process of gaining access to interviewees and survey respondents for research required us to build relationships analogous to those information security practitioners must themselves build and maintain. We recruited interviewees through conversations at information security conferences and through personal connections. Even though we assured interviewees that we would not explore sensitive topics, we had to establish a degree of trustworthiness before they would speak to us. Our affiliations with the University of California, Berkeley, and Packet Clearing House helped in this regard, establishing us as neutral researchers without malicious intent. In addition, trustworthiness was established in the course of interviews as interviewees were able to judge us for themselves. Several interviewees facilitated introductions to additional interview candidates, who themselves explicitly stated that they were talking to us only because people they trusted had vouched for us.

Figure 1: Distribution of survey respondents by age



We conducted a total of twenty-seven interviews, each lasting about an hour. Interviews were held in interviewees' offices, by video conference, or by phone, according to interviewees' preferences. Interviews were recorded with interviewees' permission and later transcribed for analysis. Our interviewees were largely from the USA, with four interviewees from New Zealand, Italy, and Norway. In spite of efforts to ensure gender diversity in our interviewee pool, our interviewees were mostly of men, with a total of four women. Interviewees covered a wide range of experience levels, from college students, to mid-career professionals, to Chief Information Security Officers (CISOs) and CEOs of information security consultancies. Our interviewee pool covered a wide variety of educational backgrounds, which appeared to have no correlation to seniority. Our interviewees ranged from CISOs who did not finish college to early career analysts who had master's degrees in computer science along with multiple information security certifications.

We designed an extensive survey, consisting of close to two hundred questions, on the basis of our analysis of interview and observational data. The survey was administered online via an anonymous link through a variety of channels. Interviewees posted the survey link to social media accounts (Twitter and LinkedIn), forwarded the survey link within their professional networks, and sent it to several email lists in which participation is restricted to vetted, trustworthy information security practitioners. In addition, we developed contacts within two professional organizations that helped distribute the survey link to their networks: Women in Security and Privacy (WISP) and the Information Systems Security Association (ISSA). Participation in the survey was incentivized by a promise to make an anonymous donation to one of several information security non-profits, which survey respondents were able to select at the conclusion of the survey (see Appendix B).

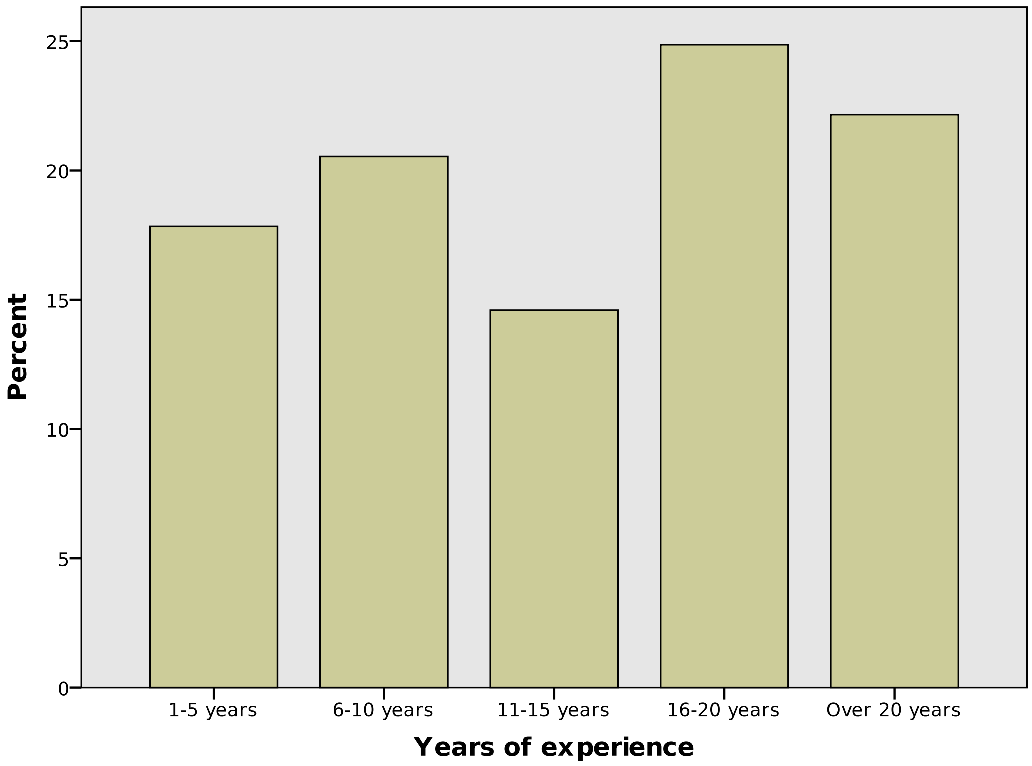
We gathered a total of 185 completed survey responses. Of these, 143 (77.3%) identified as male, 39 (21%) as female, and 3 (1.6%) as "other". Of those who identified as "other", one specified gender as nonbinary, another as genderfluid, and the third did not provide additional detail. Although low, the proportion of female-identifying respondents is better than the 11% reported in a recent industry survey.[2] Of 126 respondents volunteering their ethnicity, 105 (83%) identified as Caucasian, 9 (7.1%) as Asian, 6 (4.8%) as Hispanic, 2 (1.6%) as Black, 2 (1.6%) as Chinese, 1 (0.8%) as Arab, and 1 (0.8%) as Native American. Geographically, 138 (74.6%) of responses were from information security practitioners working in the USA, with the remaining responses from twenty-one other countries, including New Zealand, the United Kingdom, Bangladesh, Chile, and Spain. Even though our data is US-centric, the non-US representation in our data provides an invaluable additional dimension that allows us to draw conclusions about the global condition of the field of information security, by studying social relationships within and across disparate geographies. We return to the challenges of gender, race, and geography later in this report.

Survey respondents were otherwise quite diverse. They were mostly distributed across the 25–34, 35–44, and 45–54 age ranges and covered a wide range of experience in the information security industry (figures 1 and 2). The largest proportion of respondents identified as working in the Internet sector, but they also came from an array of other industry sectors (figure 3). In terms of overall job activity, a minority of 10 (5.4%) respondents grouped themselves as primarily offensive (or "red team"), a majority of 120 (64.9%) indicated that they were primarily defensive (or "blue team"), and 55 (29.7%) identified as playing both offensive and defensive roles (or "purple team"). A wide range of specific job functions was represented in the survey results (figure 4).

Although the vast majority of survey respondents had a bachelor's degree or better, almost 20% had not finished college or had graduated only from high school or a two-year associate degree program. The largest proportion of respondents who had degrees obtained them in computer science, at 42.3%. An additional 23.5% of degree holders obtained degrees in other STEM fields (including

[2] The 2017 Global Information Security Workforce Study: Women in Cybersecurity, available at https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf.

Figure 2: Distribution of survey respondents by years of experience

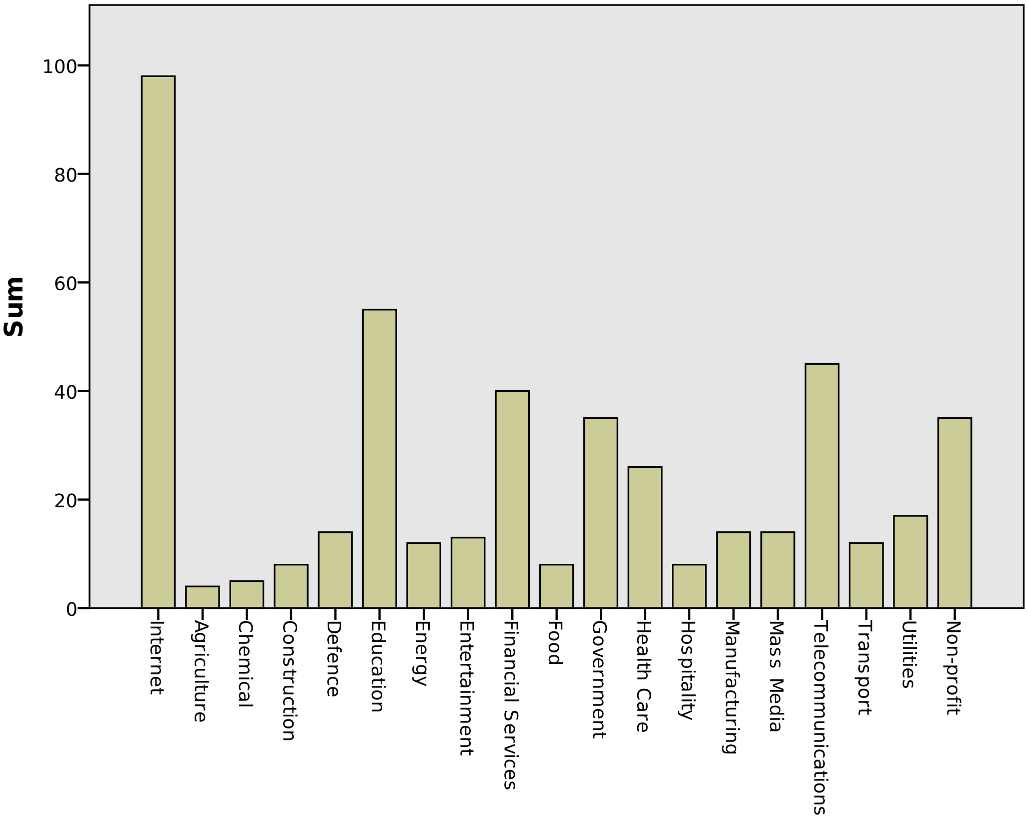


chemistry, physics, biology, engineering, earth and space sciences, and mathematics). Finally, 34.2% of degree holders obtained degrees in non-STEM fields (geography, history, law, and sociology, among others). Of all respondents, 51.9% did not hold any information security certification. Degree holders in non-computer-science fields had a slightly higher tendency to hold certifications than those in computer science fields. In general, however, degree holders were almost evenly split between those who held certifications and those who did not, regardless of the field of their degree. Of those who did not hold degrees, most also did not hold certifications (figure 5).

Our sample of interviewees and survey respondents is by no means random. We had to be able to reach interviewees and survey respondents by building connections across the fragmented communities of information security. In addition, there was an element of self-selection and motivation: interviewees and survey respondents had to be sufficiently interested and willing to make the time for participation in our research.

There were many potential participants in this research who refused to speak with us or take or distribute our survey. While distributing the survey, for instance, a contact at a large Silicon Valley company informed us that their security staff had

Figure 3: Industry sectors of survey respondents



told them not to distribute the survey within their organization, because surveys are a common vector for attacks. Related concerns arose in the course of survey distribution. Several survey respondents voiced concerns that the survey required them to enter the city and country in which they worked; they worried that these might be sufficient to identify them, along with other demographic information we collected. In response, we made these fields optional and added text to clearly indicate the reasons we were gathering this data.

In spite of these limitations, we believe that the diversity of experience levels, ages, and job activities and functions in our sample is representative of the current state of the field of information security.

Figure 4: Job functions of survey respondents

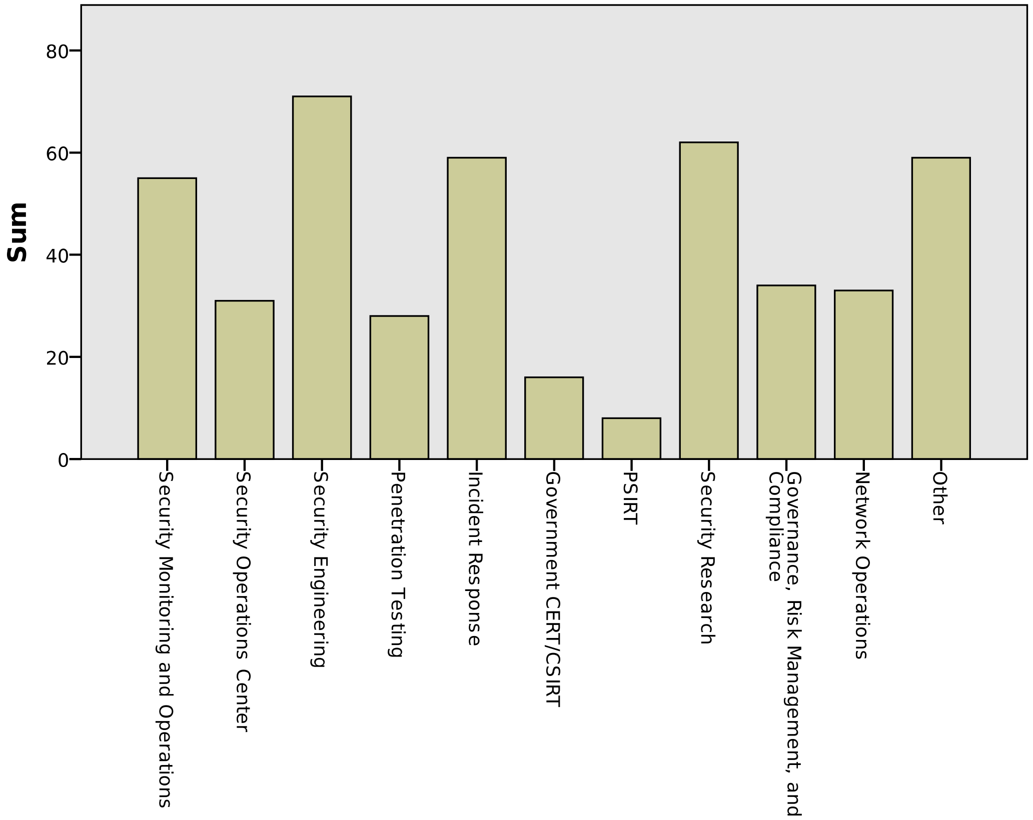
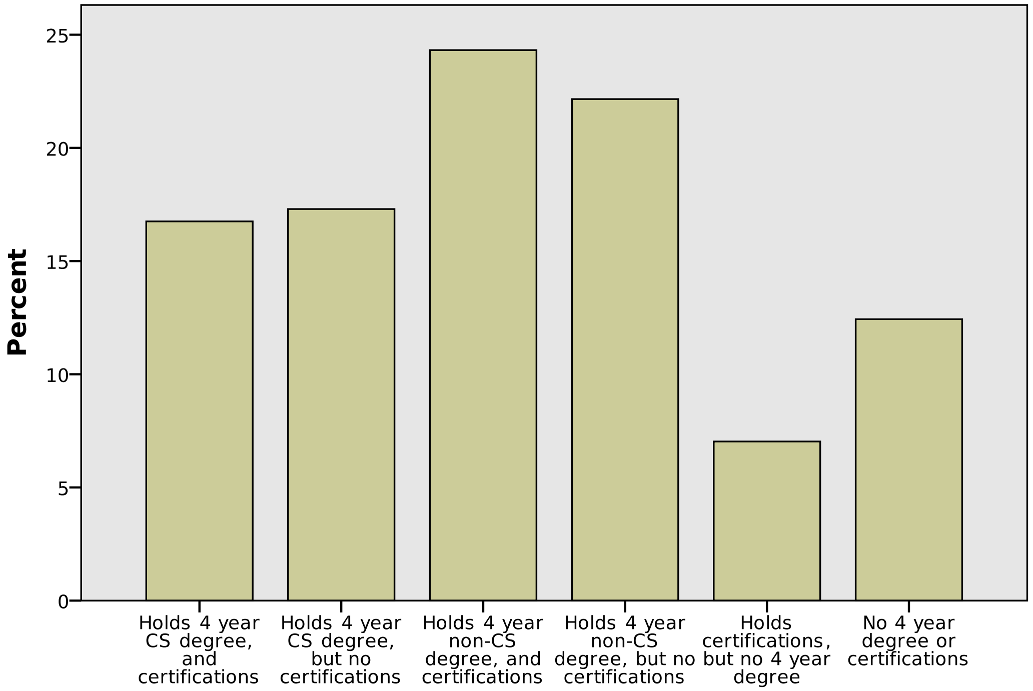


Figure 5: Distribution of survey respondents by education



3 Cooperation and Trust

Information security depends to a large degree on cooperation, especially for sharing information about emerging threats and vulnerabilities, and for sharing new techniques for responding to these problems. However, such cooperation relies upon an inherent contradiction - between protecting and sharing sensitive information that allows effective responses to the problems information security practitioners must deal with. For instance, combating a targeted intrusion to a system may require coordination with the vendors who built the system, with network providers to trace the flows of data in and out of the system, and with knowledgeable information security practitioners who have encountered similar problems. Each of these interactions embodies a set of risks, reflecting the sensitivity of the information that must be shared in order to achieve timely and thorough resolution of the problems.

> *"Cooperation relies upon an inherent contradiction - between protecting and sharing sensitive information"*

The familiar response to resolving such risks is through institutional means. CERTs or CSIRTs act as clearinghouses for threat and vulnerability information within and across countries. Sector-specific ISACs provide similar kinds of coordination functions with particular industry sectors, such as FS-ISAC for the financial services industry and REN-ISAC for research and education organizations. Some organizations may rely on third party managed security services to provide a range of information security needs. Organizations may leverage partnerships with law enforcement agencies, such as the FBI Infragard program in the USA. There is a wide range of such formal arrangements for cooperation, but in every case some kind of institutional mechanism sets rules for membership and information sharing. These institutions provide a variety of means to support cooperation, including periodic conferences, email lists for notices and discussion, and automated disclosure of threat indicators (e.g., domain names or IP addresses that are sources of attacks) via threat feeds.

These institutions work because they provide relatively closed, secure contexts for information sharing and cooperation. To gain access to the institutional networks, organizations must establish membership in the institution, whether through some kind of membership agreement or through a contractual relationship for services (as in the case of managed security services). Once membership is established for an organization, relevant personnel should be able to access the networks of cooperation and information sharing that the institution enables with personnel in other organizations.

Cooperation and information sharing do not, however, take place only through institutional mechanisms. Information security practitioners share information with trusted acquaintances to help make sense of particular kinds of problems or to coordinate responses to ongoing security incidents. Information is shared in informal settings, such as local meetups of information security practitioners. Information is shared through conference presentations and discussions, whether at open conferences that anyone may attend (e.g., DEF CON or BSides) or at closed conferences with attendance restricted to vetted organizations and individuals (e.g., M3AAWG). Indeed, when we asked survey respondents to list which conferences they attend regularly, several indicated invitation-only conferences that they could not disclose. Similarly, information is shared over open online channels (IRC, email, etc.) as well as in closed online channels restricted to vetted participants.

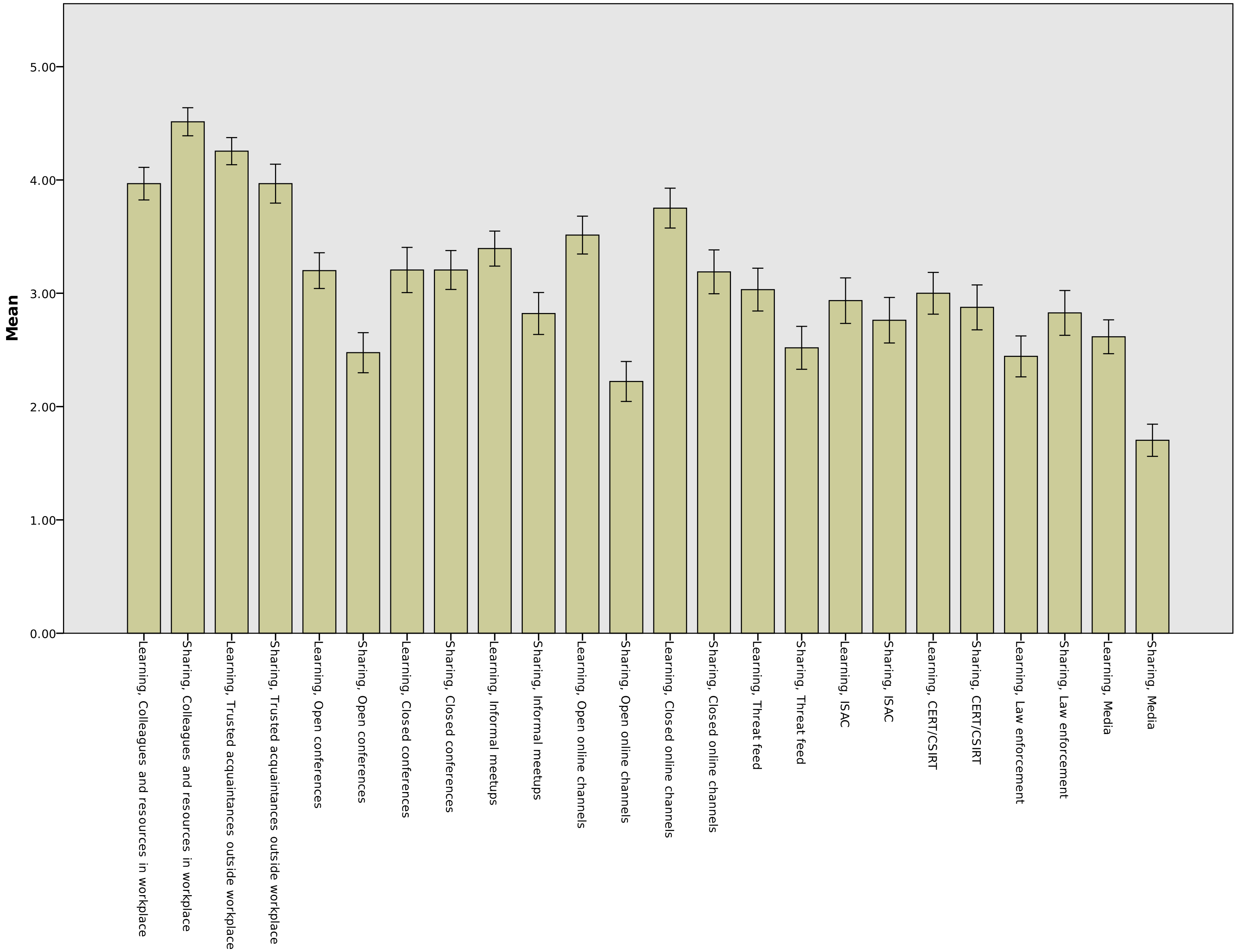
Although vetting is a necessary function of institutions for cooperation and information sharing, it does also take place outside institutional contexts. Such non-institutional vetting arrangements vary from informal groupings of acquaintances who know and trust each other to more formal groups that require one or more existing members to vouch for new members. For example, Ops-Trust is a well-known closed group for information security cooperation to which membership can be gained only by invitation from existing members. As the only public page on the Ops-Trust website notes: "Ops-T does not accept applications for membership. New candidates are nominated by their peers who are actively working with them on improving the operational robustness, integrity, and security of the Internet."[3] Across these kinds of non-institutional arrangements, membership is for individuals, not organizations, and vetting proceeds on the basis of individual reputation and trustworthiness.

We posed a series of questions in our survey to get a sense of how important different arrangements for cooperation are for *learning* about emerging threats and vulnerabilities, and new techniques for responding to these problems; and of how willing respondents are to *share* these kinds of information over these arrangements for cooperation. The results (figure 6) clearly illustrate that colleagues and resources within the workplace, and trusted acquaintances outside the workplace, are of the greatest importance for learning; and that these are also the channels across which respondents are most likely to share information. As is no surprise, organizational boundaries – within which information must be secured – function to enable intra-organizational cooperation and information sharing. Somewhat more surprising, interpersonal trust relationships – which cut across organizational boundaries – are at least as important as intra-organizational relationships for cooperation and information sharing.

Institutional mechanisms, such as ISACs and CERTs/CSIRTs, were ranked as being of moderate importance for both learning and sharing of information. Closed conferences and closed online channels (i.e., those that require vetting) promoted a

[3] See https://portal.ops-trust.net.

Figure 6: Importance of cooperative arrangements for learning and sharing information



Error Bars: 95% CI

greater willingness to share information than open conferences and online channels. In fact, open conferences and open online channels had some of the lowest scores for willingness to share information, with only the media being ranked lower. Overall, intra-organizational relationships and inter-organizational interpersonal trust relationships were of greater importance than any other mechanism surveyed for both learning and sharing of information.

This is not to say that institutional mechanisms are unimportant for learning and sharing information. Rather, we suggest, institutional mechanisms should be implemented as an important component of information sharing strategies, but viewed as a means to an end (improved information sharing) rather than an end in themselves. Viewing them in this manner allows an expansion of the scope of institutional cooperation mechanisms, recasting them as sites through which interpersonal trust relationships for cooperation may be formed as much as sites of cooperation and information sharing in themselves.

The distinction and relationship between institutional mechanisms and interpersonal trust relationships became clear in the course of our interviews. As a senior information security practitioner who has been part of FS-ISAC for many years told us:

> There are the more formal structures within the FS-ISAC where you can anonymously share information or even through the closed groups within the FS-ISAC the ability to share intelligence and have that direct.. . . It's maybe a restricted list of people which you know who's on that list. There are definitely levels of trust within there, and like with any community or any organization you use your judgment in what you want to share or maybe firm policy, as well, will dictate what you can share, with whom, when. Those are also the communities that build up and evolve over time.

When we asked what was required to gain membership in the closed groups within FS-ISAC, they responded that new members are admitted only infrequently, but that when they are:

> It's on a personal basis. There are prerequisites to being a member, but the membership of the committee is on a personal basis. What have you contributed to the field so far? What involvement have you had in the past with FS-ISAC? Those are the kinds of things that come into play in terms of making that determination. There's obviously an institutional prerequisite. You have to be a Platinum Member [of FS-ISAC] to be on the committee, but after that it's an individual decision on the person.

The institution of FS-ISAC does not obviate the need for trust relations. Rather, it provides the basic social and technical infrastructure (of conferences, email lists, threat feeds, etc.) over which interpersonal trust relationships may be formed, and within which closed, high-trust information sharing groups can emerge. Similarly, the REN-ISAC membership guidelines indicate two distinct categories of security operations representatives who participate on behalf of their member organizations. To gain access to basic REN-ISAC resources, general member representatives must be nominated by their organization and must not be rejected by the REN-ISAC community as lacking "fitness or trustworthiness." Higher levels of more secure information sharing are made available to XSec member representatives, who must be vouched for by two active XSec member representatives who "explicitly express personal trust" in the candidate.[4]

As we have already noted, interpersonal trust relationships also support a range of non-institutional mechanisms for information sharing. A senior security engineer, who has been part of various information sharing arrangements for many years, drew a strong distinction between the effectiveness of organizational and individual participation for improved cooperation:

> The thing that really was most effective was that you had someone personally vouch for each individual. It was individuals that participated, as opposed to teams. That fixed most of the problems right there.

Similarly, a security engineer at a large Silicon Valley company stressed the importance of interpersonal relationships in his account of what it takes to share information:

> I know that my colleagues, internally, they do have a very, very small list of companies that they share with. That's named individuals at known, named companies. The fact that it is small changes the quality. If you personally know every single person who is going to be reading this, and they're of a shared understanding that this is not circulated beyond the list, then that, to me, would be the precursor and a dependency for actually sharing stuff that really matters.

An interviewee who manages a security operations center echoed these concerns while explaining the rapid growth of a "trust network" of information security practitioners they are part of:

> It probably had about 120 members. It's now double that size. That does lead us sometimes to think, given that there's now 120 new members and, yes, they are connected to this trust network, but it's getting beyond the scale where we say we actually know these people personally. When you have a very fast-growing trust network, it can be very hard to maintain that initial level of trust.

[4] Quotes are drawn from the description of REN-ISAC membership criteria at https://www.REN-ISAC.net/membership/membertypes.html.

As these responses suggest, the "level of trust" and the associated willingness to share high-quality information are strongly connected to interpersonal trust relations. Access to these closed, high-trust groups is mediated through reputation and existing interpersonal trust relations. An attendee at the FIRST conference related that access to these groups – or "trust circles," as they are commonly termed – requires multiple introductions from existing members and vetting by the entire existing membership. If a member misbehaves (e.g., by inappropriately using, or publishing, information shared within the group), then not only will the misbehaving member be ejected, but those who introduced that person will be called to account and potentially ejected from the group as well. As this attendee put it, "When you introduce someone, you're staking your future on theirs." An interviewee echoed these concerns, talking about a trust circle they are part of:

> My nature, before I refer someone, I'll actually think twice. I'll only refer someone that I truly do trust. Our people's way of it is that if somebody started [laughs] leaking information out and people actually found out about it, they're like it's not only that person that will get kicked out of that, potentially the person that referred them would actually get kicked out of that as well. The information that we get through [redacted trust circle] is highly valuable, so we'll do everything we can to make sure that none of that happens.

Interpersonal trust relationships are not, of course, restricted to particular organizational groupings such as trust circles. They are born from histories of interactions across which information security practitioners have proven themselves trustworthy to one another. However, the strong sense of confidentiality within the field – required by the sensitivity of the information being shared – often calls for additional levels of vetting. As a security engineer from a large Silicon Valley company said:

> Especially within this environment, trust is everything, from people we hire, to how we approach rolling out security solutions. We will never share information to any third party that's not reputable or has a certain level of trust at all. How we define trust is the next step in that. From what I've seen, that is common relationships that people have personally at previous organizations, that may have split and done new business venture somewhere else, and maybe they're deploying a new security product. Even if that's the case, we always do a security vetting. We always try to make sure what we're getting into, we're consciously getting into by interrogating what it is that we are trying to achieve, rather than being, "Hey, you need this information. Sure, we'll give it to you."

Vetting does not apply just to arrangements for information sharing. An incident responder at a large Silicon Valley company told us how the meetups of incident responders they attend provide a "safe space" to discuss experiences:

> Meetups are a safe space because at least some security meetups are invite-only. You don't get in without going through a vetting process. It's my safe space. I'm not so much as afraid about hackers/press as I would be at DEF CON. It varies from space to space. I cannot just talk about something without checking the crowd. That comes with the nature of the work. To get into those security meetups, you have to know someone within the group. The meetup coordinators will confirm with the person who referred you. I referred a bunch of my teammates to the group, and so they would check in with me before allowing the new candidate to join the meetup group. Also, they check LinkedIn profiles to ensure if they are working in field of information security. Whenever the meetups take place, the candidates should present their company ID. They do take some precaution.

Concerns about the confidentiality of sensitive information drive information security professionals to strongly restrict their ability to discuss their problems with their peers. A senior information security practitioner, who has functioned in CISO roles in several organizations, related these concerns:

> I'll take all the information that I can collect and gather, but I am very slow to release information, and I think that that's actually one of the problems with the security community...I don't really give out information unless I absolutely inherently trust somebody with my life. Until we as a security community can overcome that, we will always be four steps behind. Those individuals that I know personally and that I have seen every single quarter for the past fifteen years, I trust them and I would share with them any threat data that I have found and I would trust the data that they shared back with me. That's the extent of the issues, is that it has to be trust gained over repeated interactions for a number of years before we feel comfortable in sharing with each other.

Interpersonal trust relationships are essential to information sharing and coordination in the practice of information security, to facilitate rapid responses to ongoing and evolving threats. As one interviewee put it, drawing an analogy to intelligence agencies:

> There's this concept that intelligence agencies and military have had for a long time of white rooms where you have two people that, in theory, cannot exchange information, because the set of policies regarding that information makes it impossible for the two agencies to actually exchange it. That information is deemed so critical and so important that they just meet and exchange it. They take the responsibility to exchange. This happens in the intelligence community all the time, for

> more and less important things. It happens in the security community very similarly. You have people that trust each other, and they know that if the other person is asking for that specific information, it's because there's something urgent that needs to be done about it. You just trust each other and give each other information.

Information security practitioners need to be able to trust their peers in order to share information for operational purposes; but, in doing so, they must remain cautious with the sensitive information being shared. We explored these contradictory impulses in our survey by using a set of validated measures to evaluate the degree to which respondents rely on trust and caution in their relationships. We used these measures to evaluate attitudes toward two social groups: (1) information security practitioners who respondents know and have worked with, and (2) information security practitioners as a whole, whether respondents know them or not. The first group provides a sense of trust and caution as applied to interpersonal relationships; the second group provides a measure of trust and caution in relation to information security practitioners in general.[5]

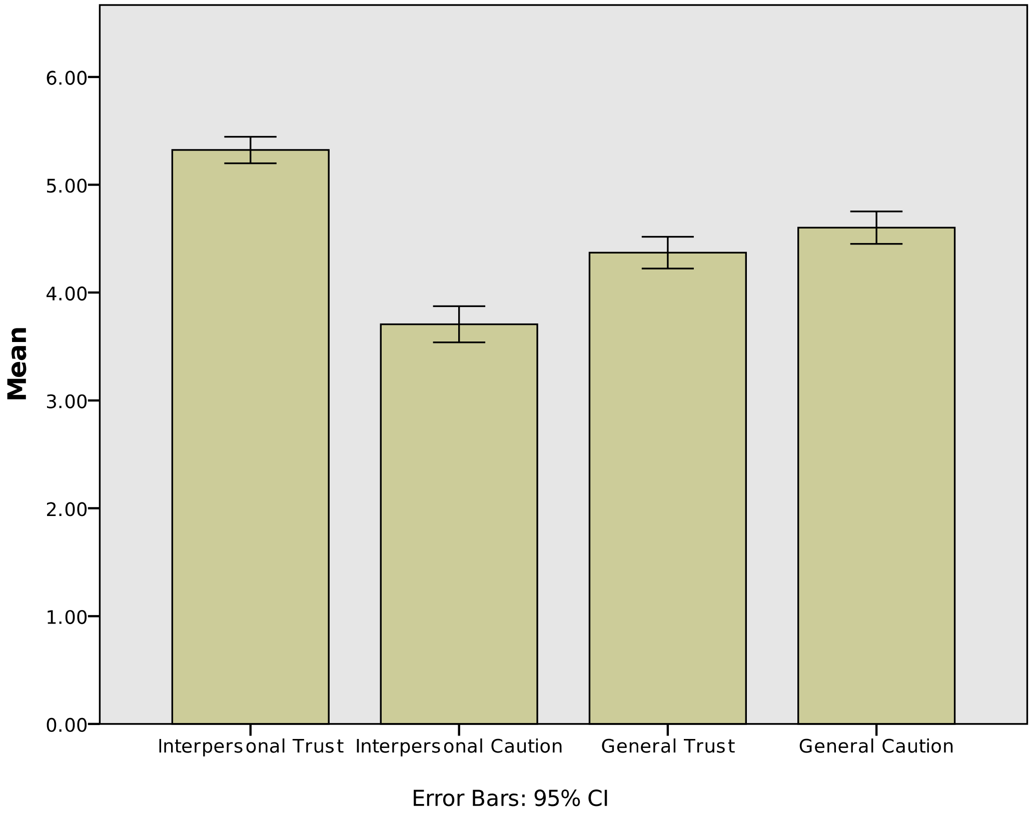
Respondents reported a high degree of trust in their interpersonal relationships with other information security practitioners (figure 7). As expected, the caution score for interpersonal relationships was lower than the trust score; when we know and trust someone, we tend to be less cautious of them. It is, however, striking that, even though the caution score was lower than the trust score for interpersonal relationships, the caution score remained relatively high overall. Information security practitioners develop strong trust relationships with their peers yet still exhibit high caution in their interactions. The contradictory impulses to secure and share information generate an environment in which cooperation tends to take place over tightly knit interpersonal relationships. The closeness of these relationships is enabled by high trust formed over repeated social interactions; at the same time, these relationships are characterized by relatively high caution to monitor ongoing cooperation.

> *"The contradictory impulses to secure and share information generate an environment in which cooperation tends to take place over tightly knit interpersonal relationships"*

The general attitudes that respondents had toward information security practitioners as a whole reflect a high degree of caution, greater than that exhibited toward interpersonal relationships. As might be expected, trust in this instance was lower than that for interpersonal relationships. However, trust was overall relatively high, about as high as caution for these general attitudes. Information security practitioners consider their peers to be generally trustworthy and are

[5] These trust and caution scales were initially developed in Yamagishi and Yamagishi (1994).

Figure 7: Trust and caution scores



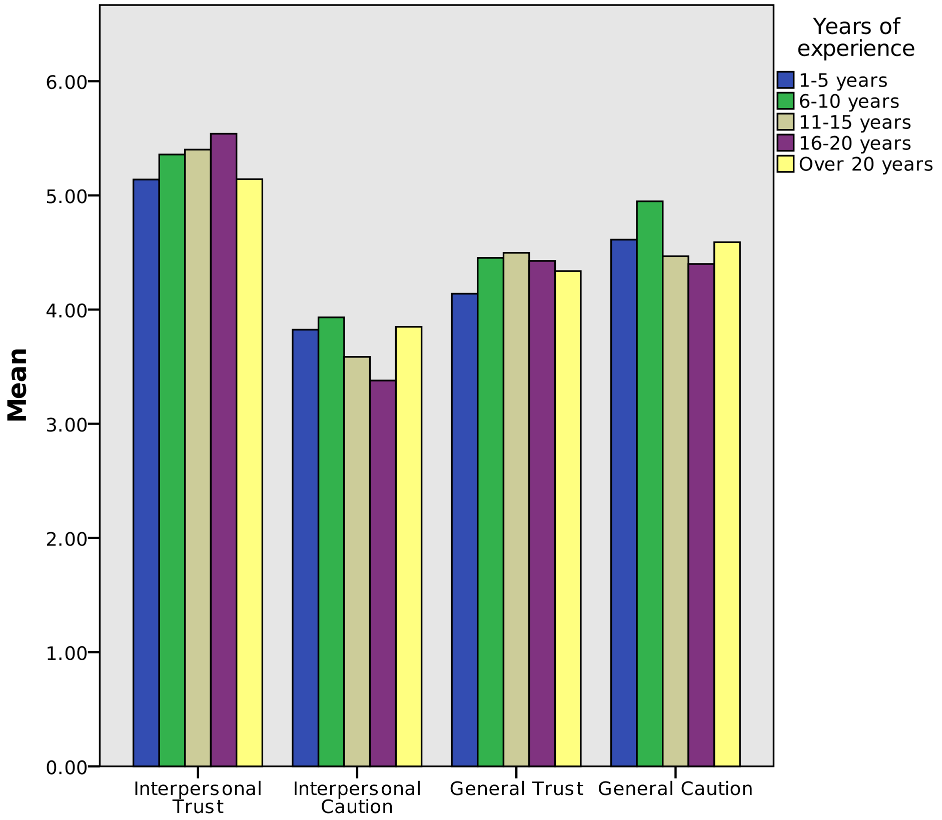
seeking to enter into strong trust relationships, but they can do so only once substantial caution has been overcome.

We found no significant variation in these trust and caution measures across a range of variables, including age, gender, and years of experience (figure 8). This lack of variation indicates that our findings represent a relatively stable set of dynamics that are characteristic of the field of information security.

Trust and caution are related, but independent, characteristics of social relationships; each contributes significantly to the bases of social interaction. A high-trust society is highly cohesive but equally highly vulnerable to disruption by malicious actors who can gain easy entry into trust relationships. A low-trust society leads to difficulties in establishing the relationships that support social cohesion and allow coordination and social exchange for the provision of societal functions (e.g., markets, governance, education). Similarly, high-caution societies generate barriers to social cohesion, just as low-caution societies are easily disrupted by malicious actors.

In general, trust and caution are inversely related. It is easy to imagine a

Figure 8: Trust and caution scores by years of experience



high-trust/low-caution society or a low-trust/high-caution society. Both conditions require strong institutions for stability. High-trust/low-caution societies require policing and regulatory institutions to guard against malicious actors. Low-trust/high-caution societies require institutionalized assurance structures (e.g., central banks that provide guarantees for the value of money in everyday exchanges) to provide support social cohesion. A low-trust/low-caution society is hypothetically possible but highly unlikely; under these conditions, people would have to be simultaneously untrusting and incautious of strangers.

The final possible condition is a high-trust/high-caution society, which is what we find in the world of information security. Information security practitioners are willing to trust their peers, but they do so very cautiously. Given that information security is by its very nature an adversarial environment, this is an unsurprising outcome. The social cohesion required for information sharing and cooperation rests upon the ability to overcome a high degree of caution.

As a consequence, all information sharing and cooperation relies upon the establishment of strong boundaries that contain the distribution of sensitive information as well as barriers to entry that restrict participation to trustworthy individuals and organizations. These boundaries and barriers serve as mechanisms to overcome caution and enable trust. Institutions – such as ISACs – provide invaluable structural mechanisms for these barriers and boundaries. It is, however, important to remember that such institutions also support the formation of interpersonal trust relationships and in fact depend upon these relationships for efficient function.

As we found, interpersonal trust relationships provide the strongest remedy for the high degree of caution among information security practitioners. Although interpersonal trust relationships are formed within institutions, they do not rely upon institutions alone. Interpersonal trust relationships are born from ongoing histories of interaction, in which individuals demonstrate their trustworthiness time after time. Such interactions may take place within organizational settings, in coordination of efforts to respond to security incidents, in conferences and information sharing groups with restricted participation, and in informal conversations (e.g., at meetups and conferences).

The disparate mechanisms (whether institutional or interpersonal) through which caution is overcome, and trust is formed, result in islands of information sharing and cooperation, which are highly connected internally but loosely connected externally. Information security practitioners deal with their high-trust/high-caution social world by constructing strongly bounded social contexts within which caution may be overcome. However, the strongly bounded nature of these social contexts equally acts as a limit on information sharing and cooperation because of the barriers that individuals and organizations must overcome to gain entry. The consequence is a loosely connected, fragmented set of social contexts that help resolve the contradictory drives toward confidentiality and interdependence characterizing the field of information security.

> *"Interpersonal trust relationships provide the strongest remedy for the high degree of caution among information security practitioners"*

Many information sharing and cooperation efforts seek to overcome this fragmentation through improved institutional mechanisms, such as government-run CERTs and CSIRTs designed to facilitate information sharing and cooperation at a national level. Although we regard such efforts as important and necessary, we argue that they are insufficient in themselves. As our findings indicate, the smaller the information sharing group, and the closer the interpersonal trust relationships, the higher the quality of information sharing and cooperation. Institutions must be understood not as an end in themselves but as a means to an end: improved relationships of trust and cooperation. As these relationships are formed and grow stronger, they create the ground upon which further cooperation may take place independent of the institutions that initially fostered them. Indeed, we argue that the success of information sharing and cooperation institutions may be gauged in part in terms of the constellation of similar arrangements which they help spawn. These arrangements take a range of forms, from informal support networks, to ad hoc working groups assembled to address particular problems, to new formal institutional arrangements, and more.

Social fragmentation is a consequence of the nature of information security. In seeking to address cooperation and information sharing across fragmented social contexts, it is important to regard fragmentation as an *intrinsic* social feature of information security, that can and should be addressed in a variety of ways.

4 Education and Learning in Practice

The field of information security has a paradoxical relationship with education. On the one hand, training programs in a variety of guises – from workshops, to certifications, to degrees – provide important support for the development of the information security workforce. On the other hand, the novelty of the problems that information security practitioners face – and the fragmented, constrained contexts within which information about these problems are shared – ensure that there can be no substitute for experiential learning in practice. The practice of information security calls for constant improvisation in response to novel threats, shaping processes of learning and thinking of information security practitioners.

The development of information security skills relies upon access to confidential knowledge that circulates in the constrained, fragmented social contexts that compose the field of information security. The process of becoming a competent information security practitioner is intimately connected with the process of building the relationships which provide access to that knowledge.

> *"The practice of information security calls for constant improvisation in response to novel threats, shaping processes of learning and thinking"*

Information security is not unique in this regard: all fields of human endeavor rely on learning by doing, through the social relationships that structure each field. Information security is distinctive in the the ways that the characteristics of the field – confidentiality, interdependence, and novelty – shape the nature of the practices and social relationships that constitute the field.

The distinction between learning in practice and formal education is made clear by two survey questions in which we sought to elicit the factors by which information security practitioners judge competence (figures 9 and 10). In the first of these questions, we asked respondents to rate the importance of different factors to competence. In the second, we asked how important different qualities are for information security practitioners. Degrees and certifications were ranked the lowest overall for judging competence. Across both questions, analytical thinking (or problem-solving ability) was ranked as being most important, followed by technical skills and curiosity.[6]

These factors – analytical thinking, technical skills, and curiosity – contribute to what we came to think of as the "security mindset," a particular way of approaching

[6] A recent survey of information security practitioners in the United Kingdom reported similar results, with respondents indicating that curiousity and practical experience are of greater importance than degrees or certification. See https://www.infosecurity-magazine.com/news/young-people-skills-gap/.

Figure 9: What makes a competent information security practitioner?

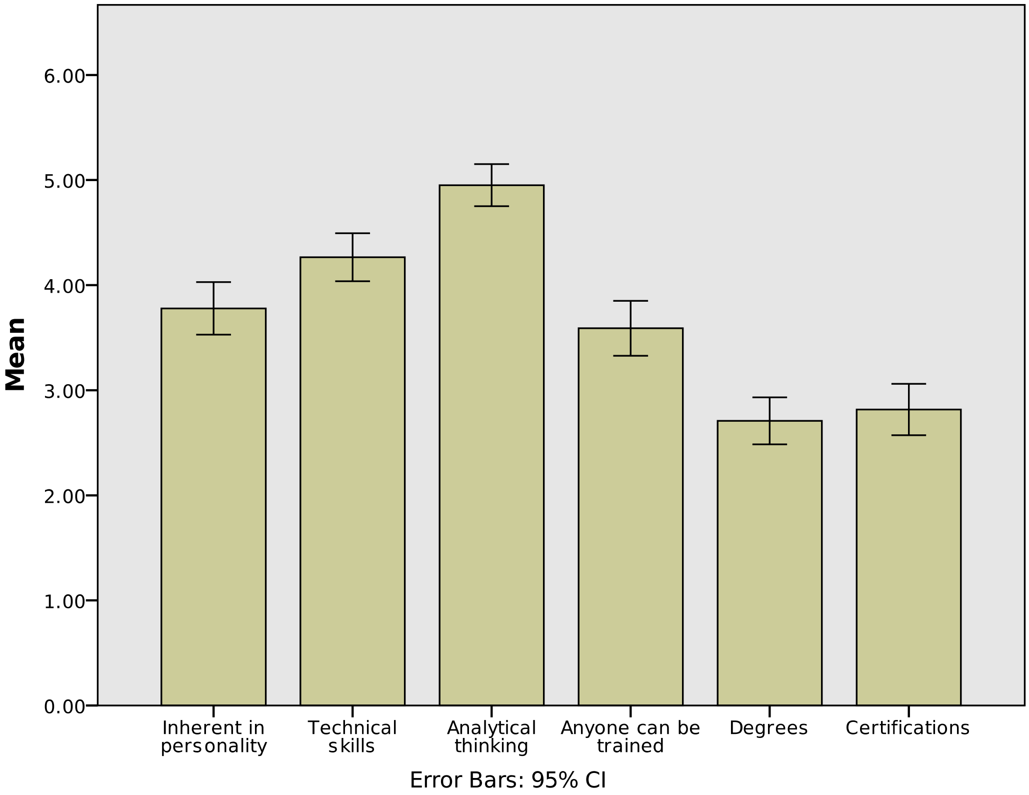
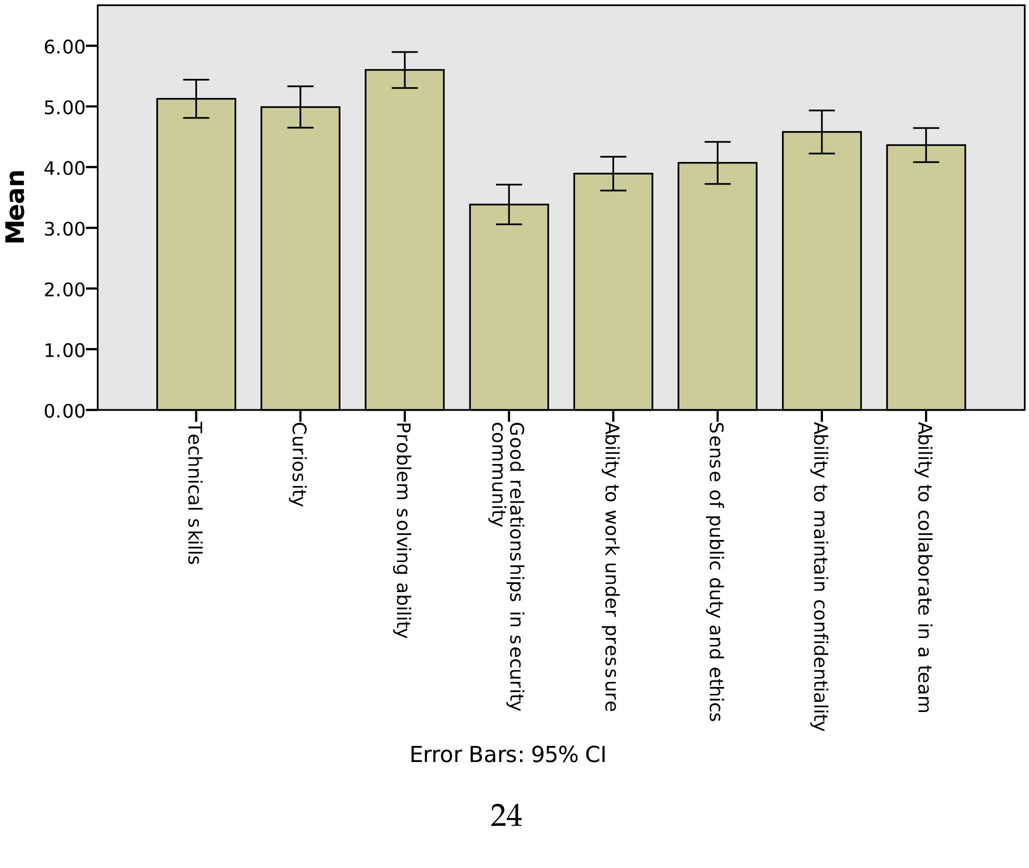


Figure 10: How important are these characteristics for information security practitioners?



problems in the world, which characterizes the field of information security.

Our survey responses indicated an almost even split between those who believed that the "security mindset" is inherent in personality and those who believed that it is something anyone can learn with training. This is an ongoing, and likely unresolvable, debate in the field of information security, but it has important implications: in growing the field of information security, should we search for people with the "security mindset" or seek to understand and train for the "security mindset"? One of our interviewees reflected on this apparent dichotomy, thinking about their own characteristics:

> I've always been intellectually curious, always challenging a little bit authority, you could say, and those skills or traits lend themselves to the field, for sure. People who are intellectually curious do seem to do well in the field, or at least can find a place in the field. I don't know how much of that is trainable...There's a certain amount of obsessive compulsiveness, as well, to the field.

An interviewee who teaches classes in information security at a university, in addition to managing a security operations center, provided a similar account:

> I think people that make good cybersecurity people are very curious. They want to know, "What happens if I type this really weird string into this field? What happens if I do this? What happens if I do that?" It's people that have a natural inclination not to always follow the manual. That is a very important personal characteristic, but I think people that are very curious and that have that curiosity, you then need to teach them a tool set. Because they do need to know a certain amount of things about network intrusion detection, about encryption, about authentication protocols, about secure coding practices, and things like that. You can then reach out I think and give them that tool set. What I've invariably found is the students that have got good futures in cybersecurity are the ones that have that curiosity and that keep poking stuff just because they want to know. On my unscientific poll I'd say of the people that I get through my class probably about 15 to 20% of them have that.

As this interviewee suggests, a basic level of technical knowledge may be teachable, but the best information security practitioners possess characteristics of curiosity and persistence. As another interviewee noted, it can be difficult to hire someone with these characteristics:

> One of the problems that I've had hiring, as well, is that if we want to hire a developer who's inquisitive and knows how to break into a web application, it's very difficult to get those two [inquisitiveness and development skills]. We're talking almost unicorn level. We've tried to

> shift a bit more to, "Is this person smart, inquisitive, and interested in development and security?" and then fill in the gaps, train them on the job. That has had mixed success.

A senior engineer at a large Silicon Valley company related a focus on characteristics of curiosity and persistence in the hiring process, to the extent of disregarding – and even negatively evaluating – degrees and certifications:

> I don't think it's a question of you're born that way, it's a question of, are you encouraged as a person to find ways around things or, are you encouraged to break things and find the weaknesses, or are you encouraged to follow instructions and go down the list and that's it? I don't put a lot of emphasis on degrees or certifications when I hire. It's a long-running, maybe not-so-inside joke that the more certifications after their name, the less qualified they are, because they want to prove that I have my certified ethical hacker and CISSP and SANS and blah, blah, blah.[7]

A senior information security practitioner in the financial services industry in New York offered a slightly different perspective on degrees, which was shared by several other interviewees:

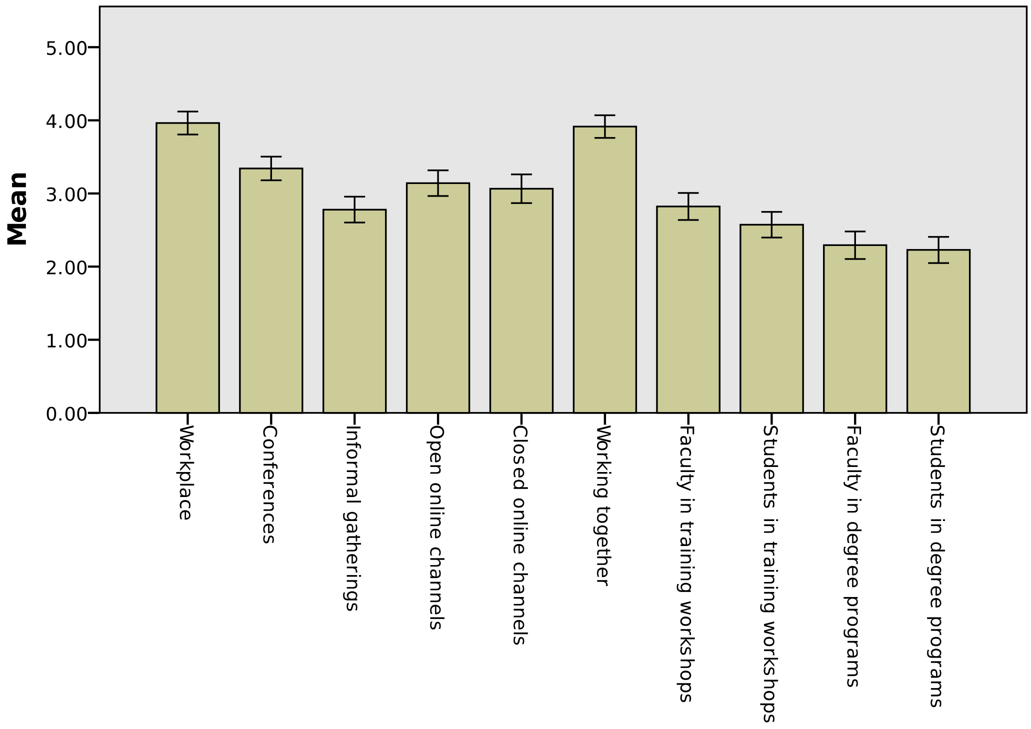
> A lot of good colleagues of mine who even to this day work in financial services, who don't have even a bachelor's degree. Definitely, I see the pros and cons. Given the field of financial services, if you don't have a bachelor's degree at least, it's an extra hoop. You need to justify why you're bringing the person in. It's also an indicator of temperament sometimes, is what I think. If you have the fortitude to be able to sit through a three-year degree that you don't want to be there for, at least you have that capacity for control sometimes, rather than being hot-headed or whatever other traits you might see out there.

Our interviewees generally did not view degrees and certifications as essential for engaging in the practice of information security. However, as the quote above suggests, degrees are viewed as means to evaluate a certain set of personality traits. Interviewees often thought the field in which the degree was obtained to be immaterial. Characteristics of the "security mindset" – curiosity, persistence, fortitude, an even temperament, analytical thinking, demonstrable technical skills – are viewed as being of greater importance for information security practitioners than markers of skill afforded by degrees or certifications.

If institutionalized education is considered to be of little value, how and where do

[7] CISSP (Certified Information Systems Security Professional) is a certification offered by the Internet Information System Security Certification Consortium (ISC)^2. SANS is an information security training institute that offers a variety of certifications.

Figure 11: Importance of social groups and contexts for learning



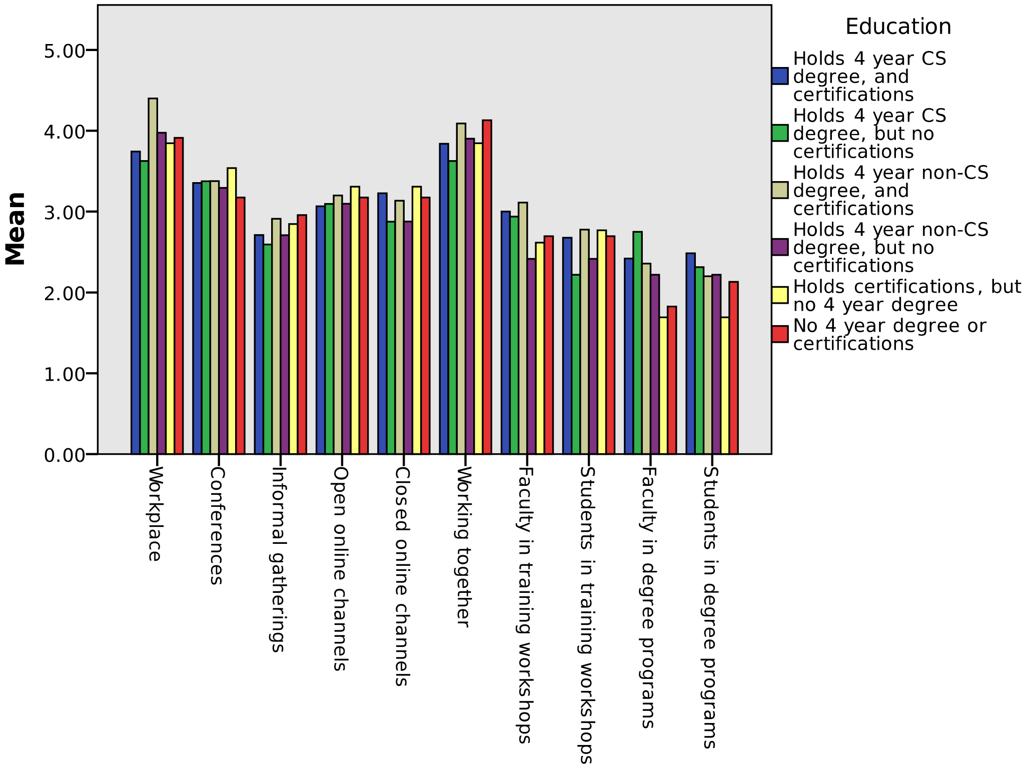
Error Bars: 95% CI

information security practitioners learn their skills? Survey respondents reported that the most important contexts for their learning were those that involve the practice of information security, in their workplaces, and in working together with their peers. Institutionalized education – in the form of degree programs – was the lowest ranked overall, scoring between just under the midpoint rating of "moderately important." Conferences, informal meetings, online channels, and workshops all scored marginally higher than degree programs (figure 11). These results were remarkably consistent, regardless of age, years of experience, gender, or educational background (figure 12).

The responses from interviewees mirrored these results and provided invaluable additional detail. Interviewees resoundingly indicated that they acquired their skills through a combination of learning by themselves from magazines and online resources and learning with others in the practice of doing security. Even in the case of learning by themselves, the online resources they made use of were produced by larger information security communities.

Although the individual experience of learning may appear to be an isolated process, it is equally an initial step toward connection to the social relationships in the field of information security, through engagement with the resources

Figure 12: Importance of social groups and contexts for learning, by educational background



constructed through these relationships. A senior information security researcher related this process of learning:

> When I had that first interview and my first job, 80% of what I knew about computers and computer security was self-taught. The other 18% was I took a couple computer science courses at my university. The last 2% I would say were from the little bit of time that I spent at SANS. Underground hacker forums, neworder.box.sk was the number one place. Lots of underground tech sites and hacking magazines, like Phrack. I would scour the Internet for the forums, the chat rooms, and the places where information was disseminated about underground hacking. I was a voracious reader. I would spend probably four to eight hours per day researching hacking. Until that point in time the grand majority of what I was learning from was self-taught. I'd never met or worked with any peers in person.

As their career progressed and they began to work with other information security practitioners and attend information security conferences, their process of learning became more reliant on interpersonal relations:

> I would say it was probably the most important part of my learning was

> meeting other people to learn from. Once I would meet somebody, I would understand what their area of specialty is, so, "Oh, yeah, you just met Sean. Sean's really, really good at hacking AIX systems, and he knows everything about those things." All right, so I put Sean in my mental Rolodex, and now, five months down the road, "Hey, Sean, I met you at DEF CON. I'm having this problem hacking an AIX system. Do you have any tips here?" That's it. That's just how it works.

A security engineer at a large Silicon Valley company provided a similar account of how in their process of learning they relied on interpersonal relationships with mentors, colleagues, and others in the field:

> For me personally, school is probably the least important. From a specific technical security engineering capacity, definitely, experience, hands-on work. Through all the mentorships I had, as well as being tasked through those mentors to learn and get hands-on technical work, that's where I've learned the majority of my stuff. Through networking, through meetups, you obviously learn as well through other people what they're rolling out. That's definitely valuable. It's really thought process as well as hands-on work that we really go over for people that are here. In fact, there are some people that we work with that haven't finished college, whatsoever.

A student in a computer science program in New York related how they became involved with a research lab at the university while they were still in high school:

> Sometimes once a week they'd have this little event called [redacted], and it was a little workshop where once a week on Wednesday evening anyone could come in regardless of whether or not you go to school, and they go over some kind of exploitation or hacking technique, the basics of it. It piqued my interest, and I started sitting in a few of them, and I didn't understand 80% of the words that they were saying. Eventually I was, "I'm real interested in this. Like, this, this seems really cool." . . . I continued being in that security lab. Now I'm actually one of the senior members. I run the workshop now.

The contrast between their opinions on the workshop and their classes was marked:

> I find classes very limiting, because they try to cater to the lowest common denominator. There is an intro-to-security class but it's very just, oh, "XSS, it's a thing! The MD5 form, it's a thing!" You think you're going to go into it more and talk about it, but no, they just move on after that. It's very shallow. It's not very practical, either, if you don't get to see it in action or do anything with it.[8]

[8] XSS (Cross Site Scripting) is a kind of vulnerability found in web applications.

They went on to relate how they've started attending conferences, like DEF CON and BSides, and started building their own relationships with other information security professionals through conversations and working on projects together.

Across all of our interviews, a common pattern repeated itself. Interviewees spoke of how they had learned their craft through a combination of self-teaching and experimentation and learning by doing in collaboration with colleagues, mentors, and other information security professionals. In these accounts, processes of learning are intricately linked with processes of establishing relationships within the communities of practice of information security. As we explained in prior sections, the relationships through which these communities of practice are constructed are trust relationships, to which access can be difficult. Similar problems of access apply to the process of learning the skills of information security, for this process too is contingent on entry into trust relationships; more sophisticated learning depends on the ability to access more sensitive information and war stories shared through strong trust relationships.

> *"More sophisticated learning depends on the ability to access more sensitive information and war stories shared through strong trust relationships."*

These dynamics were made clearest in conversations we had with a security operations center manager during the FIRST conference. They worked at a company in a small US town, distant from any major urban center, with little access to the social relationships of the communities of practice of information security. We had several discussions over the course of the conference, during which they told us that they would like to be able to publish threat information about security incidents they had experienced to some of the information sharing groups their company participated in, but were reluctant to do so. When we asked why, they responded that they weren't sure if their analysis was any good. In the absence of connections to the broader communities of practice of information security, they had no easy way to evaluate their own competence. Communities of practice are not just sites of relational learning by doing; they also help form common understandings and recognitions of competence, for oneself and for others.

It could be argued that our findings are a consequence of a field in a nascent stage of development; and that as information security matures, institutionalized education (such as that offered by degree and certificate programs) will become of greater importance. However, our research suggests that institutionalized education is currently handicapped by a disconnection from the knowledge that circulates across the social trust relationships and communities involved in the practice of information security. If conferences, informal gatherings, online channels, and workshops are all regarded as being at least as important as degree programs for learning, it is because all of these social contexts support – and are produced through – the social relationships that structure the practice of information security. In this respect, it is entirely unsurprising that workplaces and working together are viewed as being of the greatest importance for learning: both rely on social mechanisms (organizational boundaries, interpersonal trust relationships) that allow information to be shared securely. The challenge and opportunity for training the next generation of information security professionals is to build more effective connections between institutionalized education and the social relationships of practice that structure the field of information security.

5 Building Trust

If cooperation and learning in information security rely primarily upon interpersonal trust relationships, where and how do information security practitioners establish their trustworthiness and build trust relationships with their peers? We have already touched upon this question in prior sections, but it is essential to focus upon it more directly. Stronger and more widely distributed trust relationships will provide the foundation for a more competent and coordinated information security workforce and a more secure environment for everyday access to the information technology systems that structure our lives.

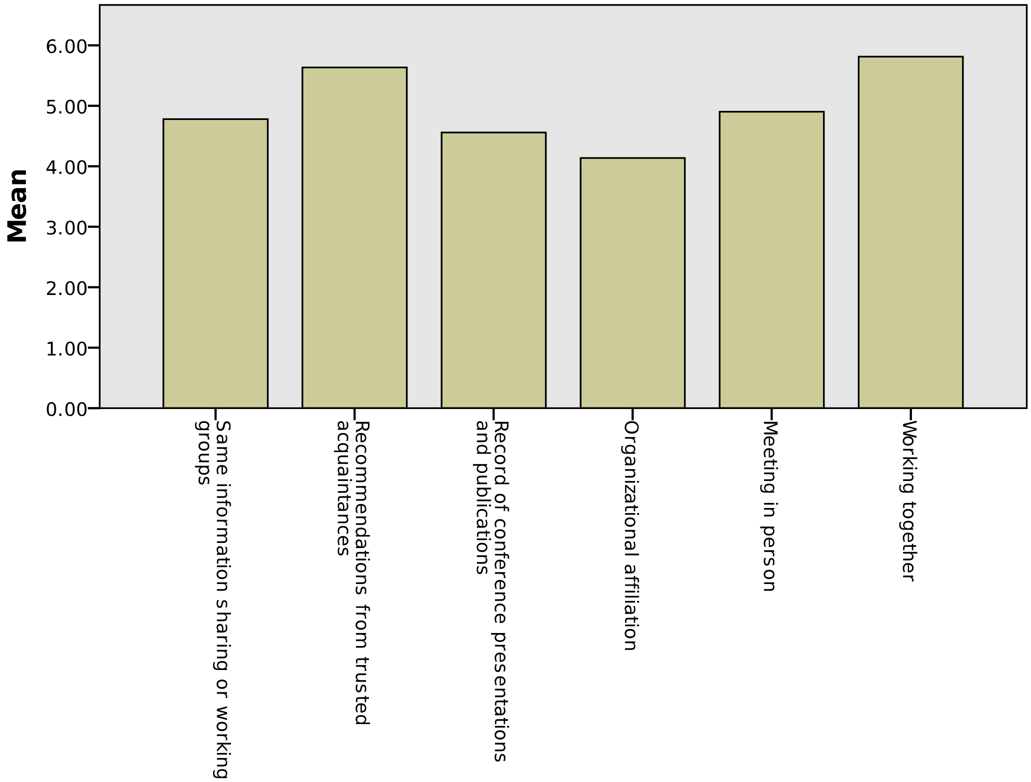
"Stronger and more widely distributed trust relationships will provide the foundation for a more competent and coordinated information security workforce"

As the trust and caution scores in our survey indicate (figure 7), information security practitioners are generally willing to trust others, but this willingness to trust is tempered by a high degree of cautiousness consistent with the sensitivity of the information that may be shared in practices of coordination for information security. A security engineer at a large Silicon Valley company reflected on the difficulty of evaluating trustworthiness and the consequent difficulties of finding entry into trust relationships in the field of information security:

> It's tough, and one of the things that you made me think of was, you need to get your foot in the door because there are a lot of so-called script-kiddies, people who don't actually want to learn security, they just want to fuck shit up. It's difficult, as a security expert, to know who to share knowledge with. It's easier if you're all sitting around in a bar. If there's some random person on the Internet, are you really going to tell this kid . . . how to exploit a SQL injection? Is that really, morally and ethically the right thing to do?

As this interviewee pointed out, meeting in person helps to establish trustworthiness, especially in social contexts where the others present are expected to have passed a certain level of vetting. As observed earlier, the social mechanisms that support such trustworthy contexts can vary from the formal vetting required for participation in closed conferences, to informal evaluations that characterize interactions at casual meetups, to recommendations from trusted peers, to a record of public presentations and publications. These kinds of social mechanisms provide the basis for evaluating the trustworthiness of potentially untrustworthy others and, in doing so, establish a means to overcome the innate cautiousness of information security practitioners.

Figure 13: How important are these factors for building trust?



Trustworthiness does not, however, equate to trust. Trust involves specific actions in specific contexts, in response to specific instances of risk and uncertainty. Security practitioners may trust each other with sensitive information in the course of coordination to resolve a particular security incident but not trust such information to other trustworthy peers outside the context of that particular interaction. Although certain aspects of security incidents may be related in the course of casual conversations within trustworthy social contexts, all of those we spoke to were clear that they were constantly on their guard, always considering how much they are able to disclose. These are not only informal social norms. They are also explicitly encoded in the FIRST Traffic Light Protocol, which defines colors that specify the contexts within which information may be shared: red for restriction to participants involved in coordination for a particular security incident, amber for restriction to participants' organizations, green for restriction to the broader community who may find the incident of concern, and white for no restrictions.[9]

Interpersonal trust relationships are strengthened over the course of repeated interactions in which peers prove themselves trustworthy to handle sensitive

[9] See https://www.first.org/tlp/.

information responsibly. These kinds of interactions necessarily take place in the practice of information security, in the context of coordination among individuals within the same, or different, organizations. Trust has a paradoxical quality to it: The formation of trust requires the taking of risks. These are typically informed risks, with information security practitioners relying on the variety of social mechanisms we have detailed to evaluate the trustworthiness of their peers. However, it is only by taking (informed) risks in sharing sensitive information, and by observing peers handing this information responsibly, that information security practitioners come to form interpersonal trust relationships.

We asked survey respondents to rate some of the factors involved in evaluating trustworthiness and building trust with other information security practitioners (figure 13). All the factors we examined were rated high by respondents; nevertheless, working together was once again rated as the most important, followed closely by recommendations from trusted acquaintances.

We encountered such concerns firsthand in the course of our research. Several of our interviewees conducted their own vetting of us prior to our interviews and told us explicitly that they had done so. These interviewees, and others, also indicated that they spoke to us only because of the channels we had come through, all of which involved personal recommendations from people they trusted. Although these recommendations were sufficient for us to gain an interview, interviewees were clear that they would not discuss sensitive topics with us. When we mentioned in the course of an interview that we had arrived at that particular interviewee after four rounds of introductions, the interviewee responded:

> That's OK. If we were to exchange some more sensitive data, probably before exchanging that, I would be calling [the person who introduced us] and asking, "OK, so you introduced me to this guy but I'm going to send him this, should I trust it to that?" I find myself, when I'm introducing people to other people for exchanging information, sending a follow-up email to the other person saying, "Hey, by the way, I met this guy at a conference. He's legit with that company, but it's not like I know him very well," just in order to clarify that my vouching reaches a certain point.

Throughout the course of our research, it became readily apparent that interactions in person are often (but not always) critical to the evaluation of trustworthiness. Most of our interviewees indicated that face-to-face interaction is essential to their process of forming interpersonal trust relations, whether in working together with their peers in the same office, by networking within their region, or by traveling to meet people at security conferences.

Information security is a global problem, so it is essential to ask how trust relationships are formed that connect information security practitioners in different countries – or even different cities in a country. An interviewee who has spent his entire career in New York and San Francisco reflected on the advantages they gained working in centers of the information technology industry:

> In New York, the people I worked with and then also the people I drank with, I would go to parties and there would be everybody who lives in the New York City area, who works in security, and there would be thirty people there. That's a really good way to get introduced. Even if you're in that sort of situation, you get some credit just from knowing somebody. Just because somebody knows me, then, obviously, I probably don't associate with idiots and so they're probably OK to talk to. . . I've been very fortunate in many ways, but also that I've lived my entire information security life in New York and San Francisco, so it's very easy for me to do that sort of thing [make professional connections].

An information security manager at a large Silicon Valley company, who moved from Seattle, spoke about the benefits of being in Silicon Valley and the geographic challenges of building relationships among information security practitioners:

> Most companies aren't in the security business but would benefit from broader efforts and would benefit from being able to share information and build relationships more easily. It also seems that a lot of that is driven by geography, that you're able to build more relationships here because you're here. If you're an ISP in middle California even, it might be more difficult. Even my buddies up in Seattle, which has a very strong security community up there, they have the same sorts of complaints. You're removed from the area down here. We can go up on the weekend or on the weekday to the city [San Francisco] and meet five people in a day. You can't pull that off [in Seattle]. The big conferences like when I'm going out to Black Hat in the next four weeks, I'm trying not to meet anyone from California. I can see them anytime. I need all my East Coast friends who I don't get to see very often or folks overseas. You try and book your dance card with them.

A manager at a security operations center in New Zealand echoed these concerns, speaking of the work they and their colleagues had to do in order to gain membership in a particular international information sharing organization:

> A lot of it was going around to find out who is actually an existing member that can vouch for us. [laughs] It's one of those trust groups that not a lot of people were aware of. We had one person that nominated us and we need two more persons to support us for us to become an official member. We make assumptions, we had to guess, to go, "Who in New Zealand is actually a member?" We actually had to

> fire off an email to go, "Hey, can you support us for that please?" Then they go, "I'm not even a member myself." [laughter] ...There was a senior member in my team. I actually hired him into the team as a junior and basically I mentored him and all that. He's one of the guys that's done really, really well. Since then he's gone over to Australia [and worked for many global companies]...Basically he's someone from New Zealand that's done really well internationally, so he's the one that I will keep in touch with, and he's the one that referred us.

Entry to this information sharing group was made possible only by the movement of a trusted colleague from New Zealand to Australia and the establishment of that colleague as trustworthy in a global context. Offices, informal meetings, conferences and other shared spaces of physical interaction provide an important foundation for trust relationships in information security. Indeed, some conferences – such as FIRST and M3AAWG – clearly state and enforce norms of confidentiality within the context of the conference. At the FIRST conference we attended, for instance, the opening plenary included this pronouncement: "No photographs during sessions, please, unless the speakers allow it. They're trying to share information with trusted parties, and we need to help them...Photos during tea breaks and socials are OK, please go ahead and put those up on Facebook!" At the M3AAWG meeting we attended, almost every presentation was prefaced with a standard slide reminding attendees not to report on the proceedings outside the context of the meeting.

"Shared spaces of physical interaction provide an important foundation for trust relationships in information security"

Physical presence is required to gain access to the information (and the trust relationships) available at these conferences. Similar concerns obtain when considering the informal spaces of interaction established at conferences. A senior security engineer related their experience of evaluating trustworthiness in face-to-face interaction at conferences:

> I have found that in small groups, at security conferences, at the bar afterwards, people tend to be very candid as long as they know that they've got a small group of a few people there. If you know who is around the table, and you have spoken to that person, you don't necessarily have to have a long-term relationship with them, but within ten, fifteen minutes you get the vibe on is this someone I think I could trust with some of this information. You don't reveal everything straight away, but we've all had war stories. We all know things go wrong.

We had firsthand experience of these kinds of interactions during our fieldwork. In the course of a conversation at the FIRST conference, an attendee began talking about research done into a particular security incident but paused, saying that they needed to think about how much detail they could actually share with us. In the context of the conference, and in being able to evaluate us in person, this attendee was willing to provide some account of a sensitive incident to us, but had to catch themselves before going further as they considered our position in relation to them. Another interviewee related similar concerns about the tensions between wanting to build new relationships and at the same time remaining cautious, reflecting on the processes through which they enter into interactions at conferences:

> If you show your affiliations toward something (say incident response or threat intelligence or a feed you follow or a bug bounty platform) and you find somebody who hates or likes them, that's a conversation starter. Vendors' drinks parties help. Alcohol tends to bring out the extrovert and the introvert in you. I've seen folks ease up a little when they meet in the casual setting. At the end of the day, we all want to make friends and share what we learned. We just don't know how to do that safely. Most of the time even with so much alcohol in somebody's system they won't give you information. I've seen that, and I'm actually proud of my industry for that.

Face-to-face interaction provides a strong basis for the evaluation of trustworthiness. Many interviewees made reference to the value they draw from the ability to judge someone from body language and facial expressions. One interviewee placed these issues clearly in the context of the practice of information security:

> As every penetration tester knows, if you want to social-engineer your way into a company, it's easier to do that electronically via emails or faxes. It's more difficult to do picking up the phone, and it's even more difficult to do that in person. I think that implicitly, since we all deal with this, and we all are trained about this, we kind of give meeting in person importance, since it takes away a lot of the possibilities of fraud and anonymity that an Internet meeting allows.

It is important to note that in-person interactions at conferences and meetups play a few distinct roles. First, larger conferences (e.g., DEF CON, Black Hat, and RSA) create opportunities for building relationships across *geographically disparate contexts*, since participants typically travel to attend these conferences; however, only a limited number of information security practitioners have the funds necessary to support such conference travel. Second, conferences and meetups promote *local* interaction, by providing a space for information security practitioners based in a particular location to meet. Finally, closed conferences and meetups provide *secure* spaces for interaction among vetted participants.

These various roles that conferences and meetups play are clearly apparent in the responses to a survey question in which we asked which conferences respondents attend regularly. Of 158 respondents who provided answers to this question, the largest proportion indicated that they attend DEF CON (37, 23.4%), followed by local Security BSides events (31, 19.6%). The fact that DEF CON and the Security BSides were the two largest proportions marks out an important set of distinctions: DEF CON is an annual conference with global attendance that provides opportunities to meet with peers from across the world, while the Security BSides are a loosely knit network of conferences organized by volunteers in cities around the world to help bring local information security communities together.[10] Respondents listed several other conferences they attended regularly, including Black Hat, RSA, FIRST, OWASP, ISACA, ISSA, and ShmooCon. In addition, several respondents indicated that they could not list the names of some of the conferences they have attended, because these are closed events in which security is in part provided by an expectation that participants do not discuss these conferences with outsiders.

In contrast to arguments about the importance of face-to-face interaction, a security researcher we interviewed spoke disparagingly of meeting in person, indicating instead that they judge others by what they are able to bring to collaborative work efforts:

> Me, I'm the person where when I was growing up, I would talk to people online all the time anyways and I had learned how to deal with people online. I'm fine with building relationships online, but not everyone has that preference. Some people are always, they're going to be socialites and they're not much more than that. They just go out there and talk to people. They know people in a shallow sense, but it's not much more than that.
>
> The kind of stuff that I do is I actually get stuff done. I'm a lot more interested in executing some plan or accomplishing something. Almost always, the people that I get to know are usually within the context of like, "Hey, I know that guy because we did XYZ together." Like that's a deep shared bonding experience that I have with most of the people that I've gotten to know.
>
> Personally, I like that approach much better than a purely social aspect of it. The people that I've met that bond over purely social non-operational type things, I generally don't like those people because they. . . How do I say why? It's almost like I see them as mostly useless because when you go out and you meet people socially, and only socially, that doesn't lead to accomplishing anything.

They also expanded on their experiences in the course of our interview, to argue

[10] For more information on Security BSides, see http://www.securitybsides.com.

that information sharing is primarily a matter of practice, in ongoing interactions between peers:

> I know that a lot of industry have been talking about information sharing in these broad, glowing terms, but in the end, the real effective information sharing is an email thread or a chat room and that's been the reality.

It is important to note that this interview was facilitated by the fact that we had met this interviewee in person at a conference, and that we had subsequently been referred by one of this interviewee's mentors. Several other interviewees provided similar accounts of collaborative work practices that rely on invitation-only online channels (e.g., email lists or IRC channels) or online work groups created specifically to address a particular security issue (e.g., taking down a botnet). Invitations to these online channels become possible as security practitioners demonstrate their abilities and trustworthiness through their work, and through conversations in more openly accessible online spaces, or at conferences. The security researcher just quoted, for instance, related that a presentation they gave at a major security conference led directly to the formation of a relationship with one of their mentors.

> *"Trust relationships are formed through cooperation in the practice of information security, whether cooperation takes place in person or through online channels"*

As these accounts suggest, although in-person interactions provide a strong basis for the evaluation of trustworthiness, trust relationships are formed through cooperation in the practice of information security, whether cooperation takes place in person or through online channels. The problem remains that access to the social relationships that constitute the practice of information security is constrained by geographic factors.

The challenges involved in evaluating trustworthiness and forming interpersonal trust relationships are endemic to the field of information security. These problems are driven by the contradictions between the characteristics of the field – confidentiality, interdependence, and novelty – and complicated further by geography. Institutions for education and cooperation provide necessary supports to help remedy these problems and contradictions. However, our research indicates that the intrinsic nature of information security is such that there can be no substitute for interpersonal trust relationships.

6 A Homogeneous Field

Issues of diversity were not central to our research design, but as our research progressed it became clear that our findings have implications for thinking about diversity, which we detail briefly in this section.

Issues of the lack of diversity, whether by race, gender, class, or other factors, plague the information technology industries, particularly in the USA. Common responses to these issues involve institutional interventions, whether in the form of affirmative action for forming more diverse student bodies at universities and more diverse workforces within companies or diversity training to create more inclusive workspaces. Though these kinds of responses are necessary for the field of information security, they may prove insufficient. The interpersonal trust relationships that structure the field of information security may constrain the efficacy of institutional interventions to support diversity. This creates a distinctive set of problems for addressing these issues.

> *"The interpersonal trust relationships that structure the field of information security may constrain the efficacy of institutional interventions to support diversity"*

Consider the sample of information security practitioners from which we drew for our research. Our interviewee pool, and survey respondents, were overwhelmingly white and male, in spite of our efforts to ensure a representation of diverse identities in our research. Indeed, we were able to increase the representation of female respondents in our survey only through our partnership with WISP. As noted earlier, our survey respondents were 77.3% male, and of those who volunteered their race 83% identified as white or Caucasian. Of our twenty-seven interviewees, only four were women, and only three were non-Caucasian. These numbers are by no means unusual; a recent industry survey suggests that women compose only 11% of the global information security workforce.[11]

We recruited interviewees through cold calls at conferences and personal introductions from prior interviewees and acquaintances in the information technology industry. The networks of relationships we followed to reach our interviewees are representative of the systems of interpersonal trust relationships we have described. In contrast, our survey respondents were recruited by more public means, through postings to mail lists and announcements on Twitter and LinkedIn by our interviewees and the organizations that supported our research. In spite of the differences between these distinct paths for recruitment of research

[11] For more information, see the 2017 Global Information Security Workforce Study at https://iamcybersafe.org/GISWS/. Data on the racial and ethnic composition of the information security workforce is forthcoming as part of a series of reports from the same survey.

participants – personal introductions vs. public announcements – we were still left with a predominantly white and male representation of information security.

We do not intend to suggest that the field of information security is composed of racists and misogynists. On the contrary, many of those we spoke with explicitly brought up these issues themselves in the course of our conversations; and these issues are very much part of the public discourse around information security. We are by no means the first to notice or to address problems of race and gender in information security.

Nevertheless, our findings on the importance of interpersonal trust relationships offer a fresh perspective on problems of diversity in the field of information security and on potential interventions to address these problems. It is well documented – and in many ways entirely unsurprising – that social networks (which rely primarily on interpersonal relationships for social cohesion) exhibit *homophily*: we find it easier to connect to people who are like us and feel less comfortable when we do not see people like us around us.[12] Homophily is not a matter merely of identity but also of the specific cultures that particular identities produce, as well as the role that identity plays in allowing individuals to feel comfortable (or uncomfortable) in such cultures. We suggest that the lack of diversity in information security may in part be caused by homophily, enabled by the interpersonal trust relationships that structure the field. This can lead to systemic – even if unconscious and unintended – bias in who enters and continues in the field of information security. Even though the field is constructed of fragmented, heterogeneous contexts, these contexts are populated by a largely homogeneous identity.

Such dynamics cannot easily be undone by purely institutional measures, although institutional measures do help. Additional interventions are required that focus on the role interpersonal trust relationships play in supporting homophily. We suggest a conscious effort to build diversity into the interpersonal trust relationships of the field, through large-scale mentorship programs, funding of scholarships to increase diversity at conferences, and other measures that will help bring people with diverse identities into the field of information security and mentor them throughout their careers in the field.

Although our analysis provides a means to account for issues of race and gender through the lens of homophily, issues of class present a distinct set of problems. We first noticed issues of class in the course of our interviews, as interviewee after interviewee related their early access to computers while growing up (regardless of age). For instance, an information security manager at a Silicon Valley company told us of his initial exposure to computers and networked systems at home in the late 1980s:

[12] As one review of studies of homophily opens, "similarity breeds connection" (McPherson et al., 2001).

> I was playing with computers from a very young age. It started with typing up simple, basic programs out of games, out of a magazine. I guess young, six, seven-year-old got exposure to a computer then. It was just very, very basic games in programming. I got into BBSes, bulletin boards, back in the day. I started running one when I was very young and it got hacked. I was like, "Oh, my goodness, how did that happen?" That was the end of the beginning for me.

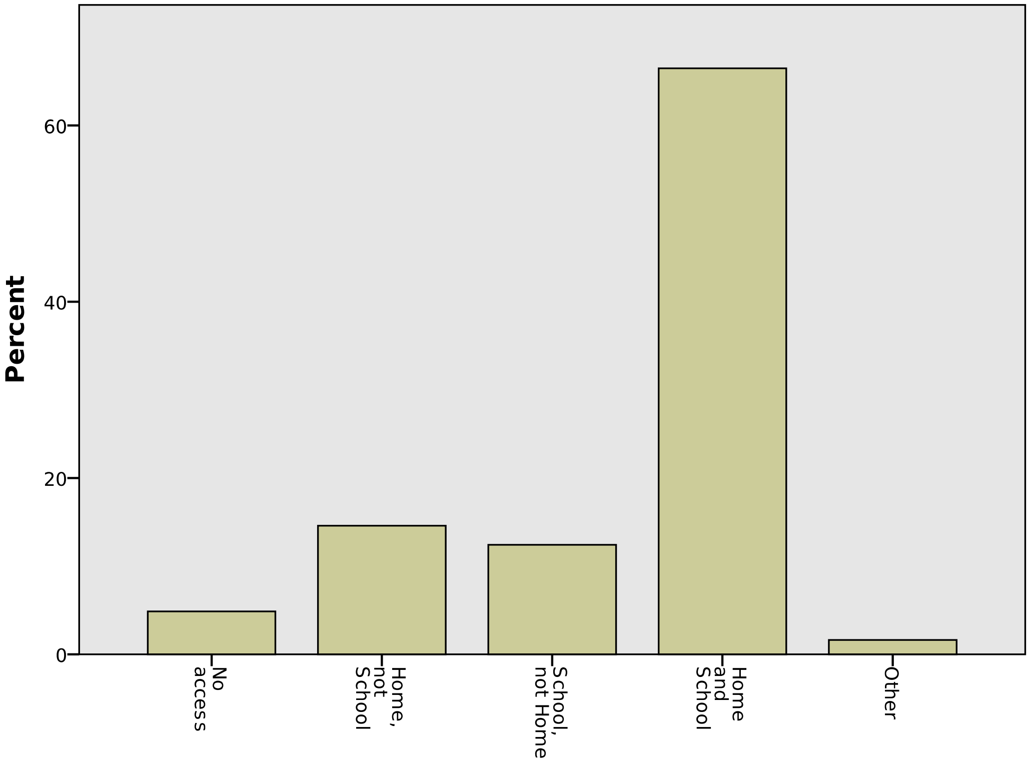
A younger interviewee, who came of age in the late 2000s, provided a similar account of his early experiences:

> I'd say it started in middle school. I was maybe eleven, twelve, something like that. It all started when I got my first smartphone. There was just something about Android, and having ability to customize all these different things, and really get the experience that you're looking for. I started to dig deeper and deeper into that, to the point where I found an online community called XDA Developers. Yeah, so they have a whole community of people making mods and custom ROMs, things like that, so I got really into that for a while. I just got more, and more curious, and eventually I started breaking things. Breaking phones and things like that. That's where I started to get more knowledge and background about the kernel, and the firmware, and different modes that the phone has, and how some of these tools get root on your phone. Things like that. That was my first exposure to the whole world of breaking things or getting unauthorized access to things.

These two accounts present distinct perspectives, on different types of devices, decades apart. But they both illustrate elements of the "security mindset" we articulated earlier, in a shared curiosity about technology. Without access to computers, and social contexts in which it is acceptable to hack computers, their curiosity about technology may never have had a chance to develop. This pattern of early access to computers was apparent from our survey data as well. The vast majority of respondents (88.1%) had access to computers while still less than 18 years of age; another 10.3% first gained access to computers in early adulthood (18–24). Of those who had access to computers while growing up (figure 14), almost all (93.5%) used computers available at home (14.6%), school (12.4%), or both home and school (66.5%).

Home computer ownership is a significant predictor of social class and is further complicated by issues that lie at the intersections of race, ethnicity, gender, and class. Consider these factors just in the USA. The 2015 report from the Pew Internet Survey indicates that, although 73% of Americans own a computer, computer ownership varies widely based on education, income, and race. Only 29% of those with less than a high school education own a computer, compared to 90% of those with a college education or better. Similarly, only 50% of those with annual incomes under

Figure 14: Where did you access computers while growing up?



$30,000 own a computer, in contrast to 91% of those with incomes over $75,000. Finally, 79% of white people own computers, as opposed to 63% of hispanic people and 45% of black people.[13]

Although these home computer ownership figures are indicative of childhood access to computers, they do not capture the kinds of social contexts that support the development of curiosity about computers through hacking. Even within households and schools that have computers, for instance, gender can strongly condition access to computers.[14] Once we consider the development of information security as a global profession, variations in access to computers and contexts of computer use across different regions and countries likely contribute to stark geographic differences in the development of the profession.

Large-scale, easy access to computers and the creation of contexts in which hacking is acceptable raise complex social and political problems. Nevertheless, we believe it is necessary to consider these as indicators for the development of a diverse and

[13] The 2015 Pew Internet Survey on Technology Device Ownership, available at http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

[14] For examples of the relationship between gender and computer access and use, see Vekiri and Chronaki (2008), Volman et al. (2005), and Barron (2004).

global information security workforce. In the short term, it may be worth considering how to consciously construct environments (from school to workplace) in which qualities of the "security mindset" – such as curiosity – are encouraged and affirmed.

Since diversity was not the principal focus of our research, our conclusions are necessarily partial and pragmatic. Further research is essential to explore and address the problems we raise in this section.

7 Conclusion and Recommendations

Current policy responses to problems of cooperation and learning in information security focus on institutional structures: improved and expanded institutions for cooperation (such as ISACs, CERTs, and CSIRTs), and improved and expanded institutions for learning (degree and certification programs). It is thought that such institutions will provide the necessary and sufficient mechanisms for enabling the inter-organizational and cross-territorial relationships required to support cooperation and learning in information security. However, as we found, cooperation and learning in information security rely on interpersonal trust relationships at least as much as on institutional structures.

Our research indicates that the importance of interpersonal trust relationships to information security is not merely a consequence of a nascent profession. Rather, we argue that this is a consequence of the interactions between three intrinsic characteristics that shape the field of information security: *confidentiality*, *interdependence*, and *novelty*. The primary task of information security is to maintain the *confidentiality* of information, as it traverses *interdependent* systems that cut across organizational and geographic contexts, in the face of ongoing, constantly evolving *novel* attacks. Due to the contradictions between these three characteristics, information security is a field composed of fragmented social contexts for cooperation and learning, with high barriers to entry. Current policy responses focus on institutional arrangements for overcoming this fragmentation. In contrast, we draw attention to the importance of interpersonal trust relationships in constituting and connecting the fragmented social contexts which compose the field of information security.

> *"Information security is a field composed of fragmented social contexts for cooperation and learning, with high barriers to entry"*

Institutional approaches to the problems of information security provide the advantage of separating the concerns of learning and cooperation. Institutions for learning can develop independently of institutions for cooperation. However, the fragmented nature of the field is a consequence of its intrinsic characteristics and is unlikely to change. Responses to the problems of information security must assume a fragmented field rather than attempt to undo fragmentation. Institutional mechanisms are often necessary to build connections across these fragmented social contexts, but they are not sufficient for this purpose. Interpersonal trust relationships provide the social connectivity to build a whole from the fragmented social contexts that constitute the field of information security.

In our research, we adopted a perspective which focuses on the *practice* of information security and the *social relationships* necessary to sustain and engage in this practice. In this perspective, learning and cooperation cannot be easily separated into distinct institutional functions. Instead, learning and cooperation must be viewed as fundamentally connected social processes which unfold together in the everyday practice of information security. Our analysis suggests a potential resolution to the apparent dichotomy between the figures of the hacker (who is born to their skills) and the engineer (who is trained to their skills), by focusing on information security practitioners as *cooperators*, who learn and engage in their practice through the relationships they build with their peers.

As we found, *trust* is the glue that holds together the fragmented field of information security. Trust in institutions and in closed trust groups formed within institutions lends value and legitimacy to institutions. Trust relationships across organizational, institutional, and geographic contexts provide the means for cross-sectoral, regional, and international responses to emerging information security threats. However, the structuring of information security through trust relationships can contribute to discrimination by race, gender, class, geography, and other markers of identity. The process of becoming an information security practitioner – of learning the skills and knowledge of information security – is inextricably linked with the process of entering into the trust relationships that structure the practice of information security.

> *"Trust is the glue that holds together the fragmented field of information security"*

In thinking about how to support cooperation and learning in information security, institutions cannot substitute for interpersonal relationships, nor can interpersonal relationships cannot substitute for institutions. It is essential to consider how to reconfigure the combinations of interpersonal relationships and institutional arrangements which together provide the social infrastructure of information security. With these results in mind, we offer a few specific recommendations for the development of the field of information security. Several of these recommendations may seem straightforward, but they are based upon insights from our research that are not immediately obvious: the connection between cooperation and learning, the contrasting and related roles of institutions and interpersonal trust relationships, and the implications of these for thinking about diversity. We believe that careful attention to these social dynamics will support thinking about policy interventions to aid the continued growth of a skilled, diverse, and effective information security workforce.

1. **Focus on interpersonal relationships as outcomes of institutions.** Institutions for education and information sharing provide invaluable supports to help resolve the problems of information security. These supports are especially important to the development of information security workforces in regions where the necessary skills and coordination

mechanisms are lacking. The success of these institutions should, however, be evaluated in terms of the networks of social relationships they foster among information security practitioners as much as in terms of the value of the specific education and information sharing services these institutions offer.

2. **Bridge fragmented circulations of knowledge with educational institutions.** Educational institutions have the potential to provide bridges to open up the circulation of knowledge and practice between the fragmented social contexts of information security. Such a bridging function relies on building relationships to these fragmented contexts and on emphasizing experiential learning through these relationships as a component of degree and certificate programs, alongside the evaluation of specific skills. Building these relationships will require a circulation of personnel between industry and educational institutions, to build the trust relationships that will sustain the circulation of knowledge through educational institutions. For instance, practitioners from the industry might act as instructors in academic programs; and institutions might focus explicitly on internships and projects that expose students to relationships within the industry.

3. **Build learning through information sharing into the function of information security teams.** As we found, organizational boundaries provide a secure environment within which sensitive information may be shared. While ongoing training is already part of many workplaces, we suggest that explicit attention to sharing the richest possible information about experiences with security incidents will provide strong support for learning within information security teams.

4. **Leverage institutional and organizational contexts to address issues of diversity.** Institutions and organizations offer critical sites from which to catalyze change within the distributed networks of interpersonal relationships which constitute the field of information security. For example, we suggest that information sharing institutions, conferences and organizational information security teams explicitly establish mentoring programs. Among the greatest challenges for new information security practitioners is that of building relationships with their peers. This challenge is magnified many times over for individuals who are of identities not well represented within the field. Individual mentoring will significantly ease the process of entry into the social relationships of the field.

5. **Increase geographic diversity through travel.** Admittedly, a significant proportion of information security cooperation takes place in purely online settings. However, as we found, face-to-face interaction is important to the formation of interpersonal trust relationships. We suggest that conferences provide scholarships to support broader regional and international attendance, potentially combined with mentorship programs. In addition, we

suggest that funding be provided to build connections between the variety of local meetups that already occur. Evidence from the network operations world (Mathew 2014) indicates that such connections between local communities are key to building a more robust operational community for global Internet infrastructure. Information security is a global problem, requiring trust relationships that span geographies as well as organizations. Travel funding will provide one pathway to help build geographically distributed trust relationships.

6. **Support local professional communities.** Localized information security meetups enhance peer networks and trust relationships. Many of these kinds of spaces have evolved organically across the world. We suggest that an explicit focus on supporting spaces for local gatherings of practitioners will be of significant benefit to the field of information security.

7. **Encourage curiosity.** Information security appears to be a calling people come to early in life, as they form a curiosity about computers through a combination of access to computers and social contexts that support hacking. It may be that the curiosity that characterizes information security practitioners is predominantly formed in youth, in which case an expansion of school computer programs may help build a future information security workforce. It is equally possible, though, that curiosity may be inculcated later in life, such as in the course of information security education programs. Further research is necessary to explore this issue, but we can suggest a focus on fostering environments that support the development of curiosity about computers in education programs, whether in high school, professional programs for information security, or the workplace. Even as education programs focus on the development of testable skills, they should equally focus upon the development of the innate qualities that characterize the "security mindset."

Information security is a remarkable field, constructed of distributed social relationships of trust as much as of institutions for education and information sharing. In drawing closer attention to the function of interpersonal trust relationships, it is our hope to contribute to the continued evolution and expansion of the field.

Appendix A: Trust and Communities of Practice

We use concepts of trust and learning in practice throughout this report. In this appendix, we provide a brief overview of these concepts and how they relate to each other for the purposes of our research. As we have argued, learning the practice of information security occurs in and through social relationships formed in the process of doing information security. Learning in this context is a situated process that occurs in social relationships constitutive of communities of practice. Following Lave and Wenger's (1991) classic formulation, the key characteristic of situated learning is legitimate peripheral participation: in order to engage in, and learn in, a community of practice, participants must be able to occupy legitimate positions to interact within the community, positions recognized by the community at large. Newcomers must be able to occupy legitimate peripheral positions, from which they may, in time, move toward more central positions. In Lave and Wenger's analysis there are no absolutely central positions in a community of practice. Rather, the positions individuals occupy are defined by their social relationships to others in the process of engaging in, and learning, their practice.

What is the nature of the social relationships constitutive of a community of practice? Lave and Wenger undertake a relational analysis to draw attention to the social relationships involved in learning, including how learning takes place in a variety of social contexts. For our analysis, we apply Lave and Wenger's theory to account more thoroughly for the nature of the social relationships involved in the communities of practice of information security practitioners.

Information security is characterized by tensions between confidentiality, interdependence, and novelty. These tensions can be articulated in terms of risk (Cook et al. 2005): How likely is it that a system might be compromised? What resources are needed to guard against system compromise? Investments in information security teams are driven by risk calculations. Decisions to share – or not share – information to resolve problems in interdependent systems may be framed in terms of perceived risk. All exceptions to expected behavior of systems constitute risks in themselves.

Responses to risk may be analyzed in terms of two opposed forms: assurance structures and interpersonal trust relationships. Assurance structures provide warrants to enable multiple parties to engage in potentially risky social interactions, with confidence that institutions will take on the burden of risk (Giddens 1990; Luhmann 1979; Yamagishi and Yamagishi 1994). Assurance structures may be formal organizations, such as central banks that warrant the value of money, or normative structures, such as patterns of expected behavior within a community.

Repeated exchanges within a given context can over time lead the parties involved to overcome their sense of risk, by forming interpersonal trust relationships (Hardin 2002). Choice is integral to trust. In the absence of choice (you do not get to choose your central bank, for instance), one may have confidence in an assurance structure, but one cannot trust it. The formation of trust relationships implies an ability to choose whether or not to enter into the interactions that may be facilitated by those relationships (Luhmann 1988). In practice, ongoing, stable social interactions in risky contexts are made possible by a combination of assurance structures and interpersonal trust relationships (Cheshire 2011; Mathew and Cheshire 2017).

Trust is as much a matter of individual attitudes and cultural dispositions as it is of social structures of interpersonal relationships and assurances. It is important to evaluate the degree to which people are willing to trust others and, equally, the degree to which people are cautious in their interactions with others. Individual attitudes of trustfulness and cautiousness evolve alongside structures of interpersonal relationships and assurances to shape social interactions in risky contexts. We evaluated attitudes to trust and caution in our survey using the scales initially developed in Yamagishi and Yamagishi (1994). The ten-item trust and caution instrument asks five questions about whether participants think that most people are basically honest and trustworthy (trust) and five items about whether one can avoid problems by guarding oneself against the negative intentions of others (caution). The trust and caution scales and metrics developed by Yamagishi and his colleagues have been applied to a variety of communities, including general research participation (Fiore et al. 2014), online dating (Fiore et al. 2010), and experimental comparisons between different cultures and societies (for a review, see Yamagishi 2011).

As Yamagishi (1998) argues, high general trust implies a belief in the benevolence of others' intentions, whereas low general trust indicates an inclination to adopt a more skeptical view of others. Yet high general trust is not necessarily the same as gullibility (Yamagishi et al. 1999). In fact, discretion and caution toward others are both highly related to trust, but they are independent concepts (Yamagishi and Yamagishi 1994). Higher general trust is sometimes associated with lower dispositions to be cautious of others, and individuals with high trust and low caution are more likely to engage in a wider variety of risky but potentially profitable and beneficial interactions (Yamagishi 2001). Overall, the dimensions of trust and caution are important for examining a variety of social relationships where risk and uncertainty are central to decision making.

The nature of responses to the risks inherent in information security define social relationships within the communities of practice of information security practitioners. Trustworthy assurance structures may reduce the need for interpersonal trust. For example, reputed degree or certification programs could provide a basis for entry into the communities of practice of information security.

Equally, interpersonal trust relationships formed in the process of doing information security may enable individuals to present themselves as trustworthy participants in the communities of practice of information security.

We intentionally use the plural "communities of practice" rather than "community of practice" in our analysis. As we have shown, high-quality information sharing, and associated, sophisticated learning in practice, rely on interpersonal trust relationships – rather than assurance structures – in the communities of practice of information security. Because the risks involved in information security are so high – and often difficult to measure meaningfully – information sharing (and associated processes of learning) takes place over strong trust relationships within situated, bounded contexts. In contrast to commonly accepted, "warmly persuasive" (Williams 1985, 76) notions of community, which emphasize openness and inclusion, the field of information security is constituted of multiple, variegated, overlapping communities defined by their internal trust relationships, to which entry can be difficult. The challenge to assuming legitimate peripheral positions from which to participate in the communities of practice of information security lies in overcoming barriers to entry by demonstrating trustworthiness and forming interpersonal trust relationships.

Appendix B: Donations

As thanks for participating in the our survey, we offered survey respondents an opportunity to select an organization to which we would make a donation on their behalf from a pool of USD 5,000. Based on our survey respondents' votes, we made the following donations:

Organization	Votes	Donation
Electronic Frontier Foundation	81 (56.67%)	USD 2833.50
Open Rights Group	10 (6.99%)	USD 349.50
Derechos Digitales	4 (2.80%)	USD 140.00
Information Systems Security Association	9 (6.29%)	USD 314.50
Women in Security and Privacy	34 (23.78%)	USD 1189.00
Open Web Application Security Project	5 (3.50%)	USD 175.00

Although the Linux Foundation was on the list of organizations for donation, they no longer offer an option for direct donations. As a result, we have proportionately split the donation amount among the remaining organizations. One survey respondent asked us to direct a donation to an organization not named in our survey, the Rural Technology Fund. We have directed USD 30 to this organization.

Bibliography

Barron, Brigid. 2004. "Learning Ecologies for Technological Fluency: Gender and Experience Differences." *Journal of Educational Computing Research* 31 (1): 1–36.

Cheshire, Coye. 2011. "Online Trust, Trustworthiness, or Assurance?" *Daedalus* 140 (4): 49–58.

Cook, Karen S., Toshio Yamagishi, Coye Cheshire, Robin Cooper, Masafumi Matsuda, and Rie Mashima. 2005. "Trust Building via Risk Taking: A Cross-Societal Experiment." *Social Psychology Quarterly* 68 (2): 121–42.

Fiore, Andrew T., Coye Cheshire, Lindsay S. Taylor, and G. A. Mendelsohn. 2014. "Incentives to Participate in Online Research: An Experimental Examination of 'Surprise' Incentives." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 3433-3442.

Fiore, Andrew T., L. S. Taylor, X. Zhong, G. A. Mendelsohn, and C. Cheshire. 2010. "Who's Right and Who Writes: People, Profiles, Contacts, and Replies in Online Dating." In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Honolulu, HI, USA.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Stanford University Press.

Hardin, Russell. 2002. *Trust and Trustworthiness*. Russell Sage Foundation Publications.

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

Luhmann, Niklas. 1979. *Trust and Power*. John Wiley and Sons.

—. 1988. "Familiarity, Confidence, Trust: Problems and Alternatives." In *Trust: Making and Breaking Cooperative Relations*, edited by Diego Gambetta, 94–107. Basil Blackwell.

Mathew, Ashwin Jacob. 2014. *Where in the World Is the Internet? Locating Political Power in Internet Infrastructure*. Ph.D dissertation, University of California, Berkeley. http://www.ischool.berkeley.edu/research/publications/ashwin_mathew/2014/where_world_internet_locating_political_power_internet_infrastructure.

Mathew, Ashwin Jacob, and Coye Cheshire. 2017. "Risky Business: Social Trust and Community in the Practice of Cybersecurity for Internet Infrastructure." In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2341–50, Waikoloa, HI, USA. http://hdl.handle.net/10125/41438.

McPherson, Miller, Lynn Lovin, and James Cook. 2001. "Birds of a Feather: Homophily in Social Networks." *Annual Review of Sociology* 27 (1): 415–44.

Vekiri, Ioanna, and Anna Chronaki. 2008. "Gender Issues in Technology Use: Perceived Social Support, Computer Self-Efficacy and Value Beliefs, and Computer Use beyond School." *Computers and Education* 51 (3): 1392–1404.

Volman, Monique, Edith Van Eck, Irma Heemskerk, and Els Kuiper. 2005. "New Technologies, New Differences: Gender and Ethnic Differences in Pupils' Use of ICT in Primary and Secondary Education." *Computers and Education* 45 (1): 35–55.

Williams, Raymond. 1985. *Keywords*. 2nd ed. Oxford University Press.

Yamagishi, Toshio. 1998. *The Structure of Trust: The Evolutionary Games of Mind and Society*. University of Tokyo Press.

—. 2001. "Trust as a Form of Social Intelligence." In *Trust in Society*, edited by Karen S. Cook, 121-147. Russell Sage Foundation Publications.

—. 2011. *Trust: The Evolutionary Game of Mind and Society*. Springer Science and Business Media.

Yamagishi, Toshio, M. Kikuchi, and M. Kosugi. 1999. "Trust, Gullibility, and Social Intelligence." *Asian Journal of Social Psychology* 2 (1): 145-161.

Yamagishi, Toshio, and Midori Yamagishi. 1994. "Trust and Commitment in the United States and Japan." *Motivation and Emotion* 18 (2): 129–66.