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

Executive Summary

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

Read the full report at https://www.pch.net/resources/Papers/A_Fragmented_Whole/

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.

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/.

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. It is also a challenge to build the information security teams required to mount these responses, as there are insufficient numbers of trained information security professionals to staff these teams.

At first glance, the problems of cooperation and learning seem unrelated; in fact, current cybersecurity policies treat them as independent problems to be addressed through institutional means. 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. Similarly, institutional mechanisms for learning – such as certificate and degree programs – are essential for training and credentialing information security practitioners for entry to the job market.

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

In contrast, our research indicates that cooperation and 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. In general, our research juxtaposes *interpersonal relationships built on social trust* with *institutional arrangements* for cooperation and learning in information security.

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 security evolves, institutional arrangements will provide long-term solutions to the problems we raise. However, our findings indicate 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.

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

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. Through our analysis of this data, we came to understand that 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.

Social fragmentation is a consequence of the nature of information security. In seeking to address cooperation and learning across fragmented social contexts, it is important to regard fragmentation as an *intrinsic* social feature of information security, that can and should be addressed through combinations of interpersonal trust relationships and institutional arrangements.

2 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, such as CERTs, CSIRTs, ISACs, and law enforcement. 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 via threat feeds.

These institutions work because they provide relatively closed, secure contexts for information sharing and cooperation. To gain access to an institutional network, 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 or at closed conferences with attendance restricted to vetted organizations and individuals.

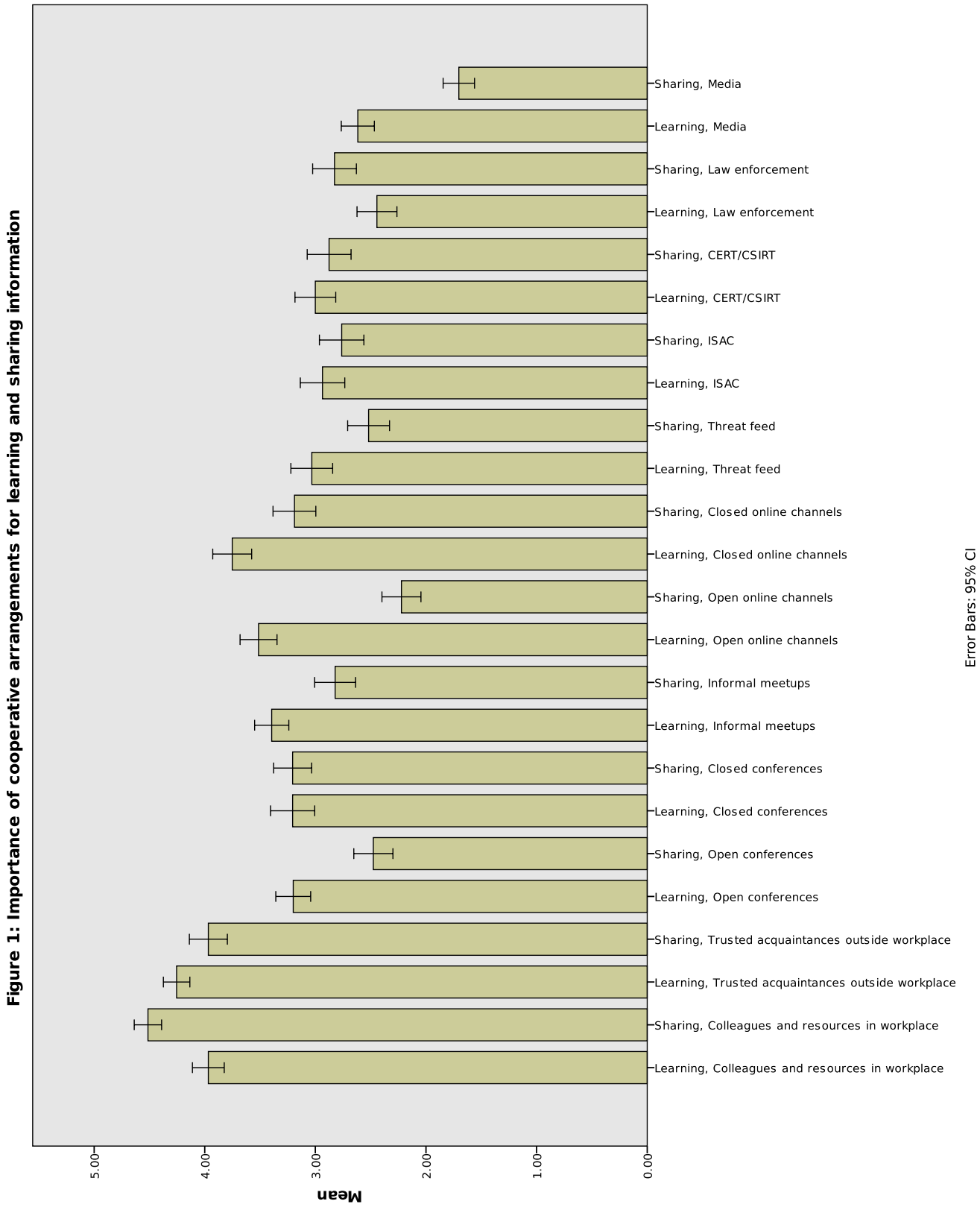


Figure 1: Importance of cooperative arrangements for learning and sharing information
Sharing, Media
Learning, Media
Sharing, Law enforcement
Learning, Law enforcement
Sharing, CERT/CSIRT
Learning, CERT/CSIRT
Sharing, ISAC
Learning, ISAC
Sharing, Threat feed
Learning, Threat feed
Sharing, Closed online channels
Learning, Closed online channels
Sharing, Open online channels
Learning, Open online channels
Sharing, Informal meetups
Learning, Informal meetups
Sharing, Closed conferences
Learning, Closed conferences
Sharing, Open conferences
Learning, Open conferences
Sharing, Trusted acquaintances outside workplace
Learning, Trusted acquaintances outside workplace
Sharing, Colleagues and resources in workplace
Learning, Colleagues and resources in workplace
Mean
5.00
4.00
3.00
2.00
1.00
0.00
Error Bars: 95% CI

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 1) 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 surprisingly, 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 CERTs, CSIRTs, and ISACs, 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 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.

The disparate mechanisms (whether institutional or interpersonal) through which risk is overcome, and trust is formed, result in islands of information sharing and cooperation, which are highly connected internally but loosely connected externally. The strongly bounded nature of these social contexts acts as a limit on information sharing and cooperation because of the barriers that individuals and organizations must overcome to gain entry. The result is a loosely connected, fragmented set of social contexts which are a consequence the contradictory drives toward confidentiality and interdependence in information security. Effective cooperation across these fragmented social contexts requires thinking about social mechanisms which reconfigure and combine institutional arrangements and interpersonal trust relationships.

3 Education and Learning in Practice

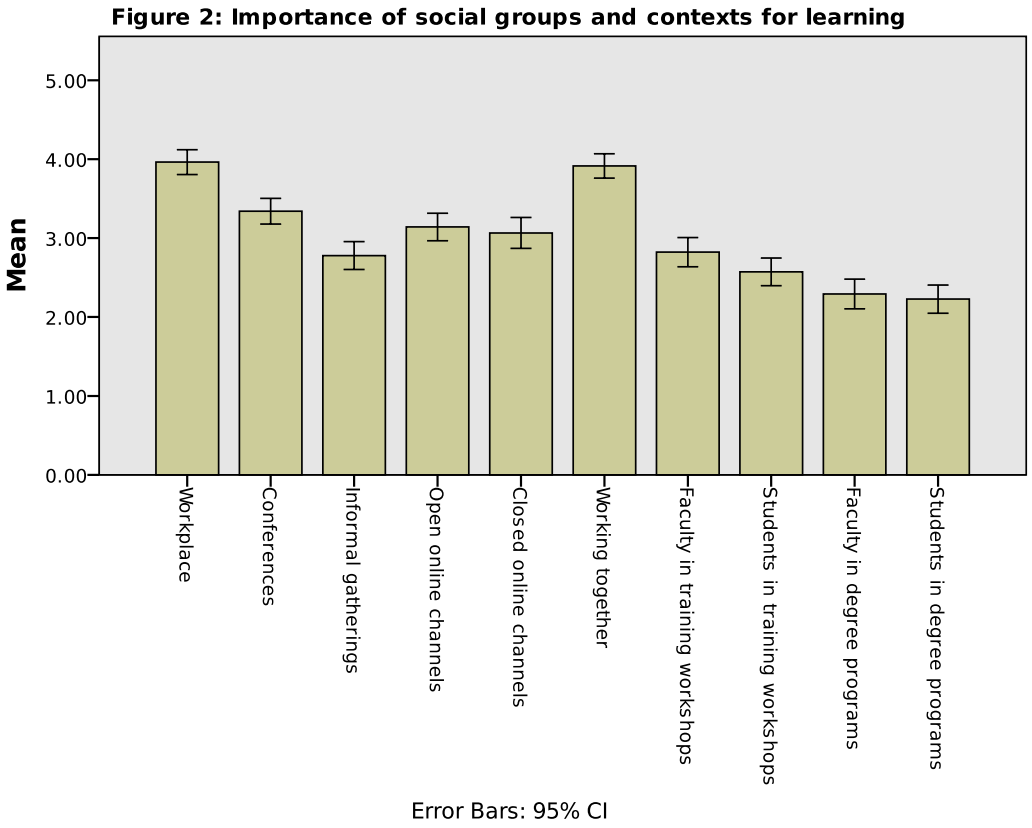
The field of information security has a paradoxical relationship with education. On the one hand, training programs in a variety of guises – from workshops, to certifications, to degrees – provide important support for the development of the information security workforce. On the other hand, the novelty 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"*

The distinction between learning in practice and formal education is made clear by a survey question in which we asked respondents to rate the importance of different social groups and contexts for their own learning. 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 2). These results were remarkably consistent, regardless of age, years of experience, gender, or educational background.

Similar themes were readily apparent in our interviews. 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. 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.

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.

4 Conclusion and Recommendations

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, as we found, cooperation and learning in information security are connected problems that depend upon interpersonal trust relationships at least as much as upon institutional structures. Cooperation and learning in information security take place across loosely connected, fragmented social contexts that are a consequence of the intrinsic characteristics of the field. Responses to the problems of information security must assume a fragmented field rather than attempt to undo fragmentation through purely institutional mechanisms.

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. 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 the full report, we detail the social mechanisms involved in building and maintaining trust. We also explore the implications of our findings for diversity in information security, by gender, race, class, geography, and other markers of identity.

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. Building these bridges 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.

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 field of information security. 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. 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.** As we found, 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 which 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.

Read the full report at
https://www.pch.net/resources/Papers/A_Fragmented_Whole/