Cooperation and Learning in Information Security
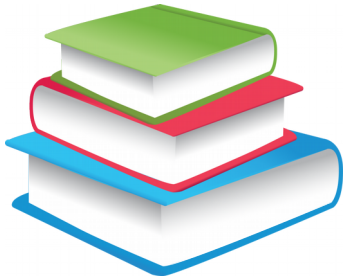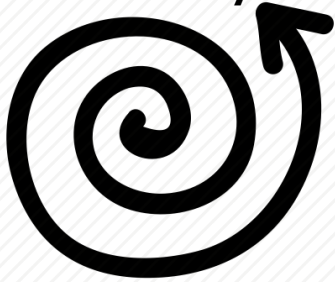
Ashwin J. Mathew
ashwinjmathew@berkeley.edu

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

PCH
Packet Clearing House
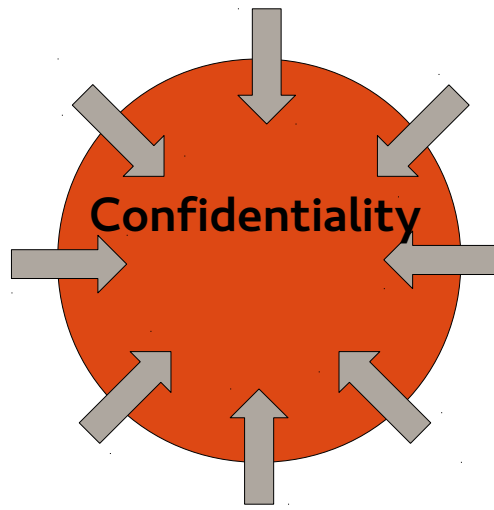
Institutional Solutions
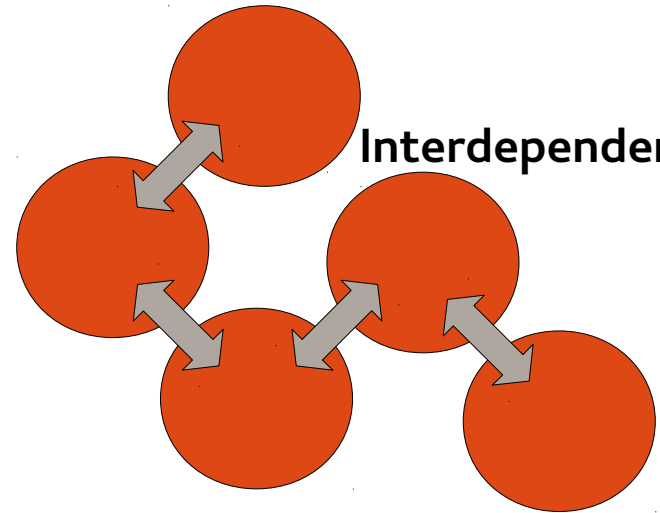
Learning

Novelty

Degrees
Certifications
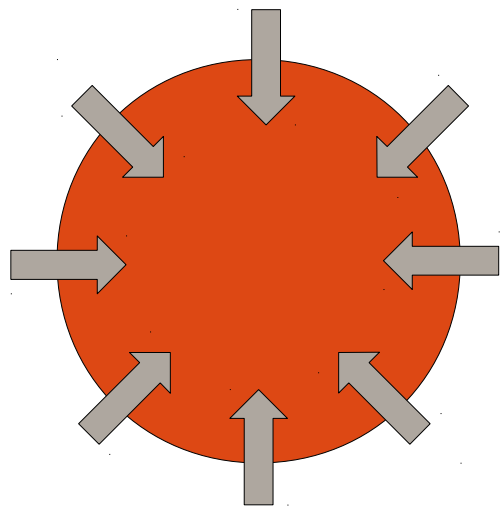
Confidentiality

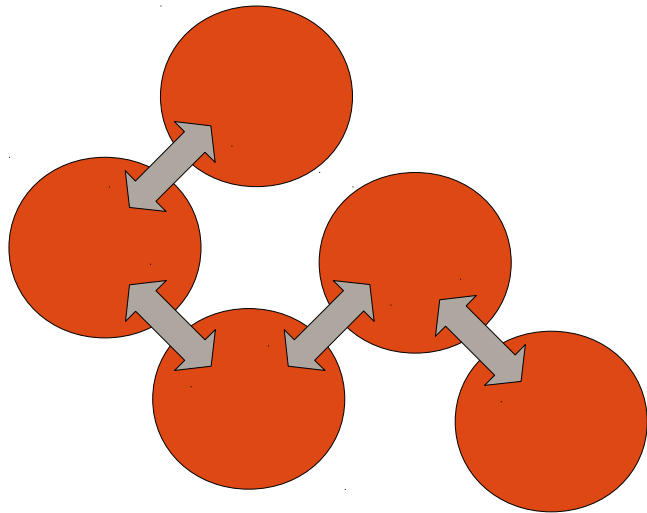## Cooperation

Interdependence

Information
Sharing
+
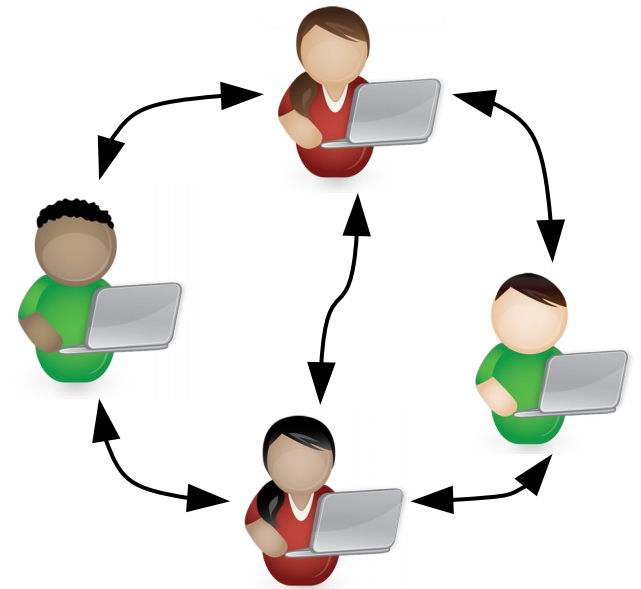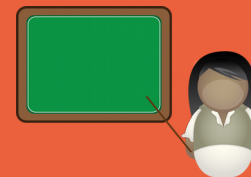Coordination

CERT
CSIRT
ISAC
Law Enforcement
...

Confidentiality

Interdependence

Novelty

Interpersonal Trust

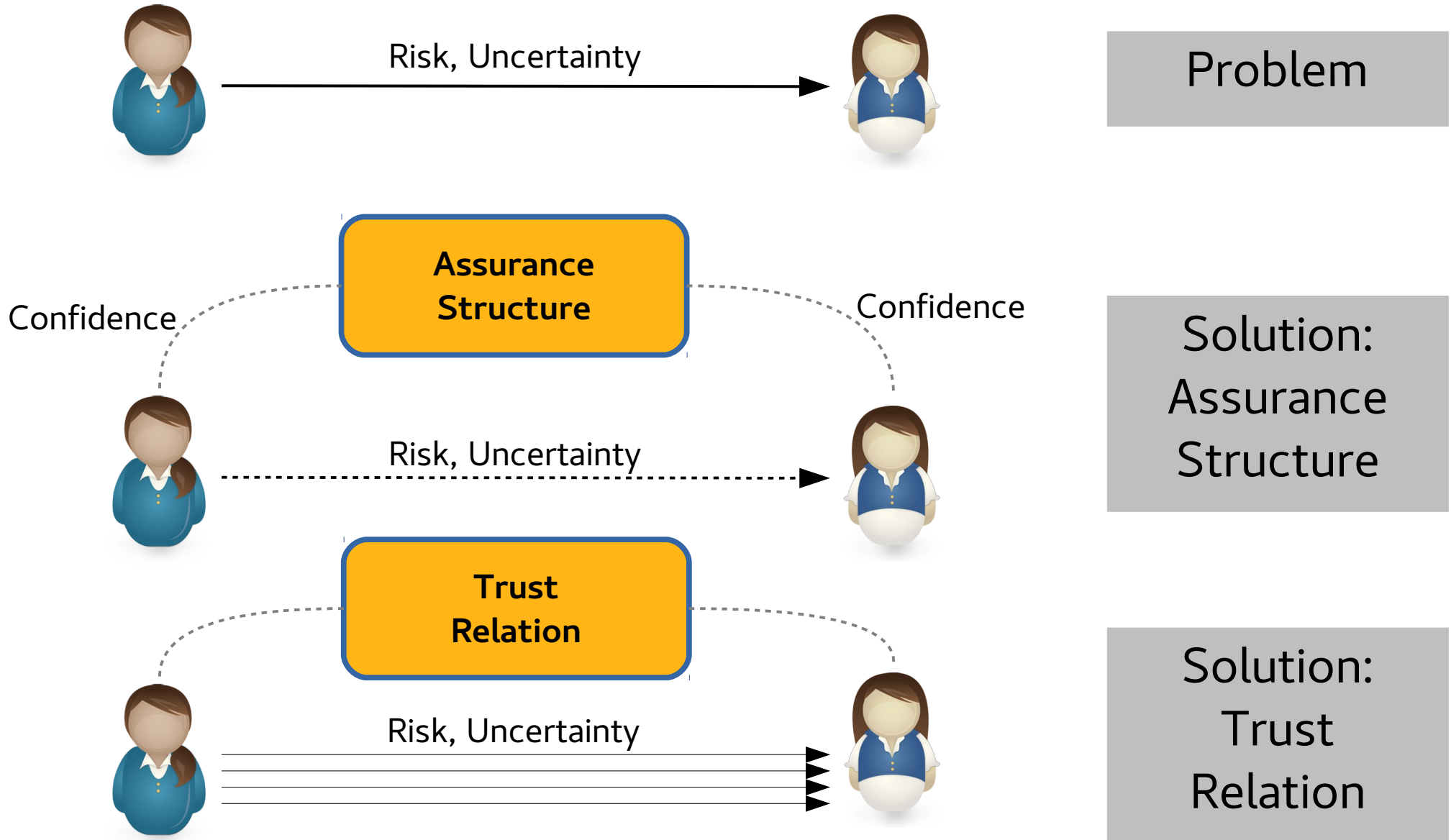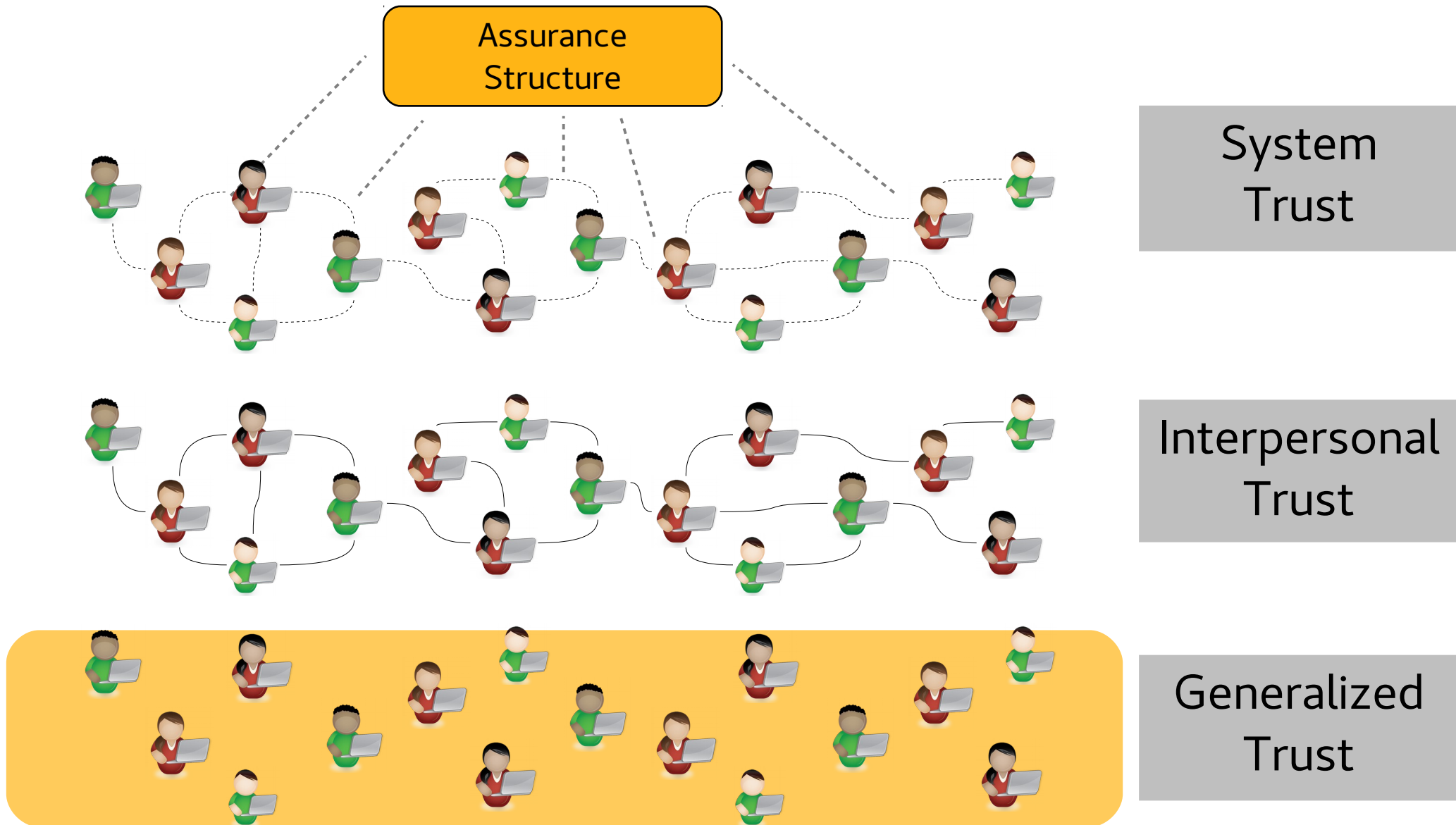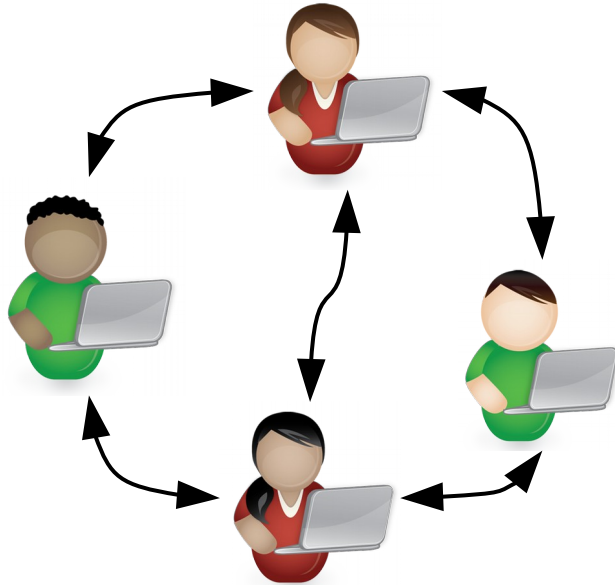Communities of Practice

Models of Trust

Risk, Uncertainty

Problem

Assurance Structure

Confidence

Confidence

Risk, Uncertainty

Solution: Assurance Structure

Trust Relation

Risk, Uncertainty

Solution: Trust Relation

Trust in Society

Interpersonal Trust and Cooperation

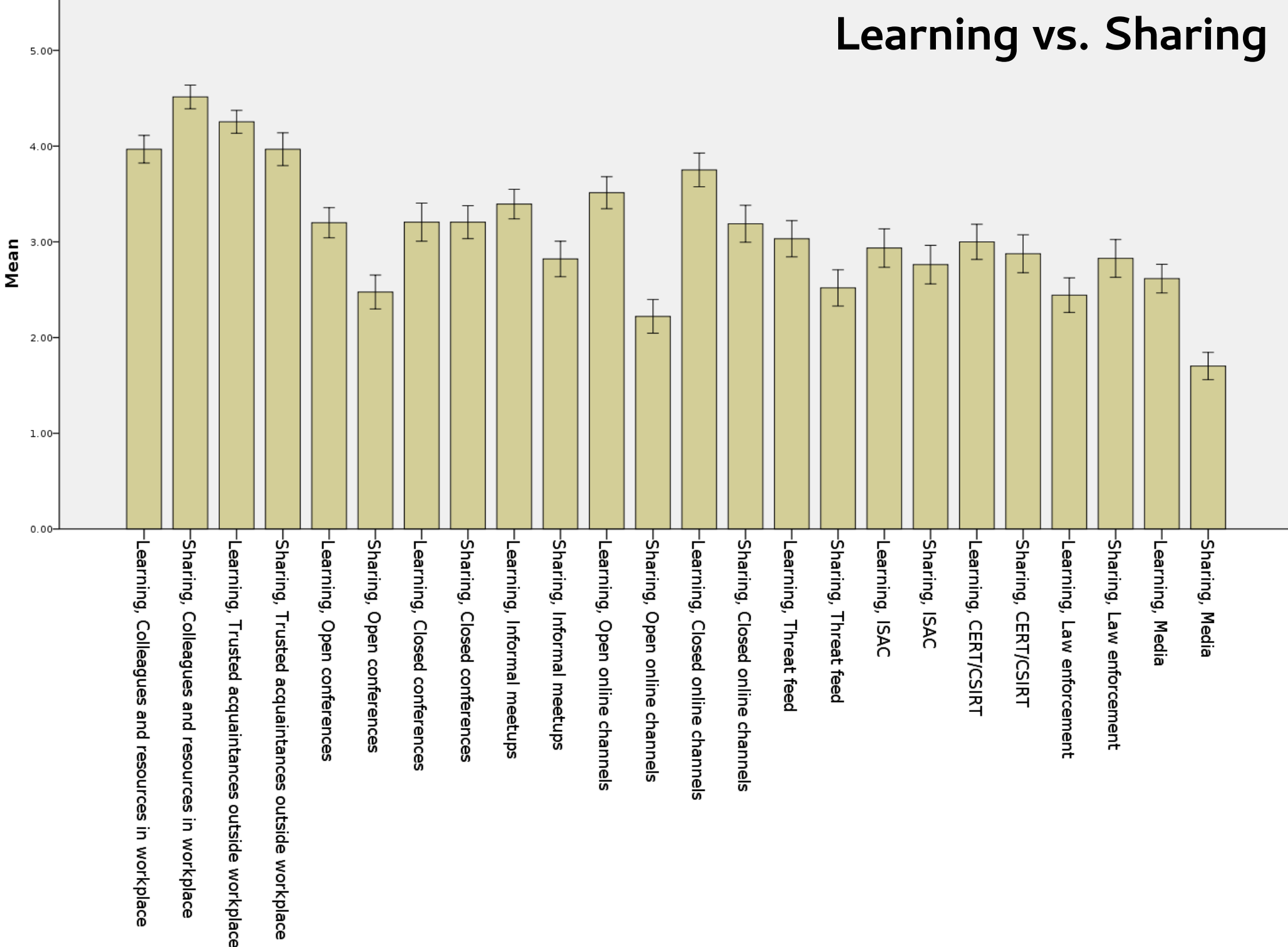Constrained circulations of knowledge and practice

Especially within this environment, **trust is everything**, from people we hire, to how we approach rolling out security solutions.

I'll **take all the information** that I can collect and gather, but I am very **slow to release** information... I don't really give out information unless I absolutely inherently **trust** somebody with my life... it has to be trust gained over **repeated interactions** for a **number of years** before we feel comfortable in sharing with each other.

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.

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.
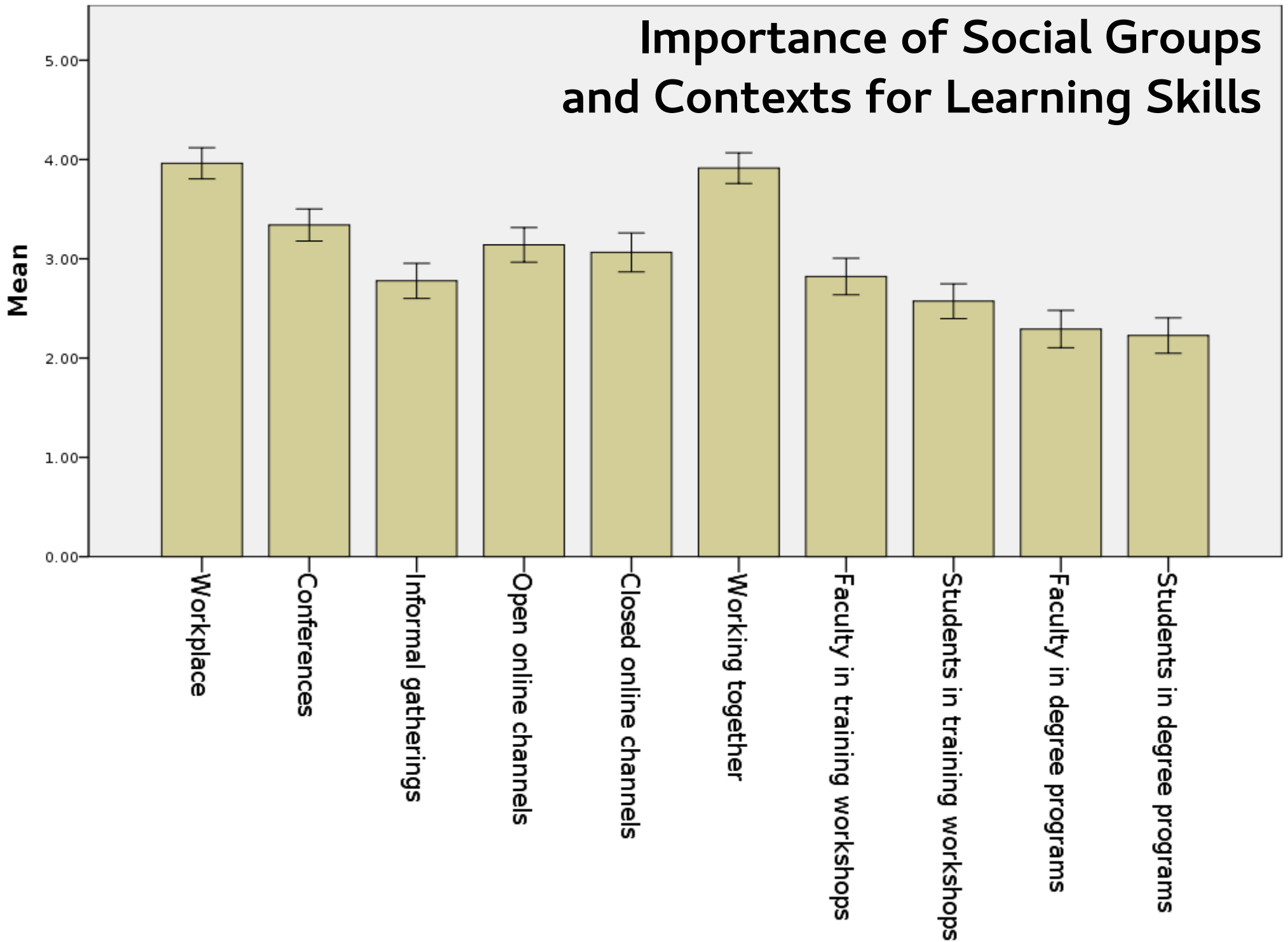
Learning vs. Sharing

Error Bars: 95% CI

Mean

5.00 — 4.00 — 3.00 — 2.00 — 1.00 — 0.00

Categories (left to right):
- Learning, Colleagues and resources in workplace
- Sharing, Colleagues and resources in workplace
- Learning, Trusted acquaintances outside workplace
- Sharing, Trusted acquaintances outside workplace
- Learning, Open conferences
- Sharing, Open conferences
- Learning, Closed conferences
- Sharing, Closed conferences
- Learning, Informal meetups
- Sharing, Informal meetups
- Learning, Open online channels
- Sharing, Open online channels
- Learning, Closed online channels
- Sharing, Closed online channels
- Learning, Threat feed
- Sharing, Threat feed
- Learning, ISAC
- Sharing, ISAC
- Learning, CERT/CSIRT
- Sharing, CERT/CSIRT
- Learning, Law enforcement
- Sharing, Law enforcement
- Learning, Media
- Sharing, Media

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 leaking information out and people actually found out about it, they're like it's not only that person that will get kicked out, 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.

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.

Importance of Social Groups and Contexts for Learning Skills

Mean

5.00

4.00

3.00

2.00

1.00

0.00

Workplace
Conferences
Informal gatherings
Open online channels
Closed online channels
Working together
Faculty in training workshops
Students in training workshops
Faculty in degree programs
Students in degree programs

Error Bars: 95% CI

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 meet-ups, you obviously learn as well through other people what they're rolling out.

When I had that first interview and my first job, 80 percent of what I knew about computers and computer security was **self-taught**. The other 18 percent was I took a couple computer science courses at my university. The last two percent 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.
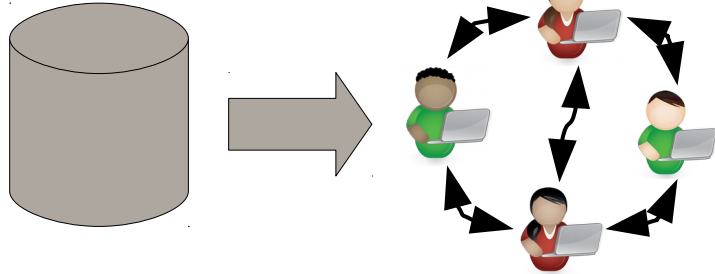
A Fragmented Field

A Fragmented Field
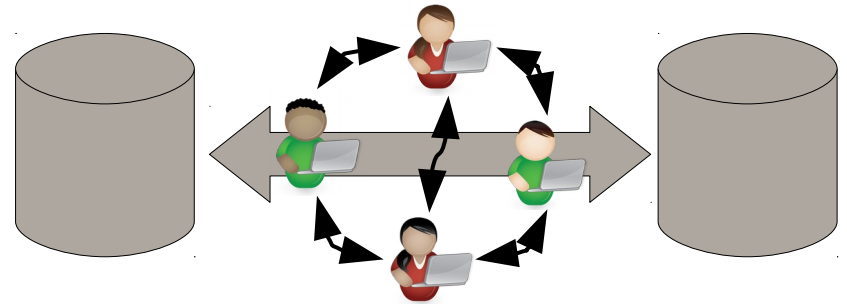
Confidentiality

Interdependence

Novelty
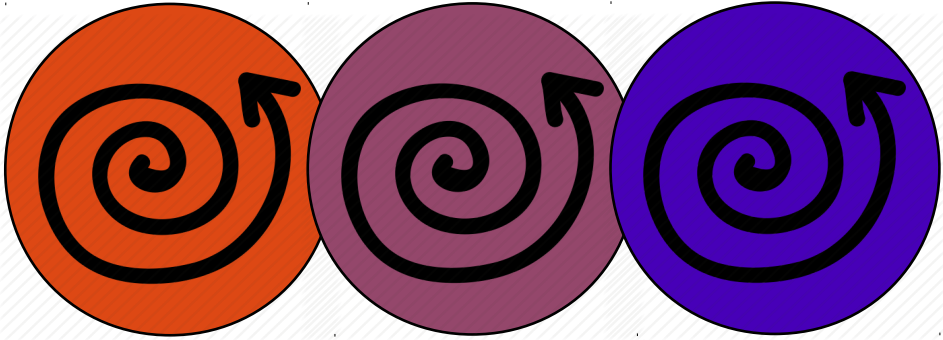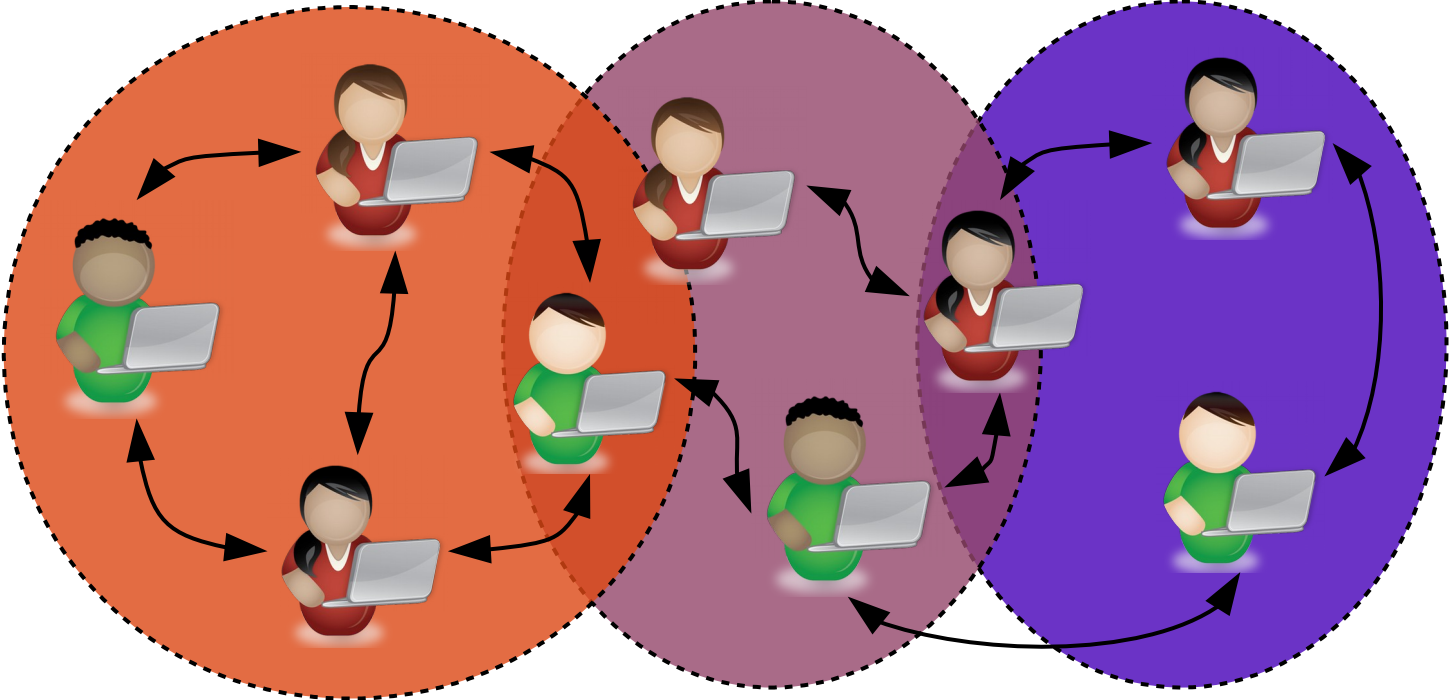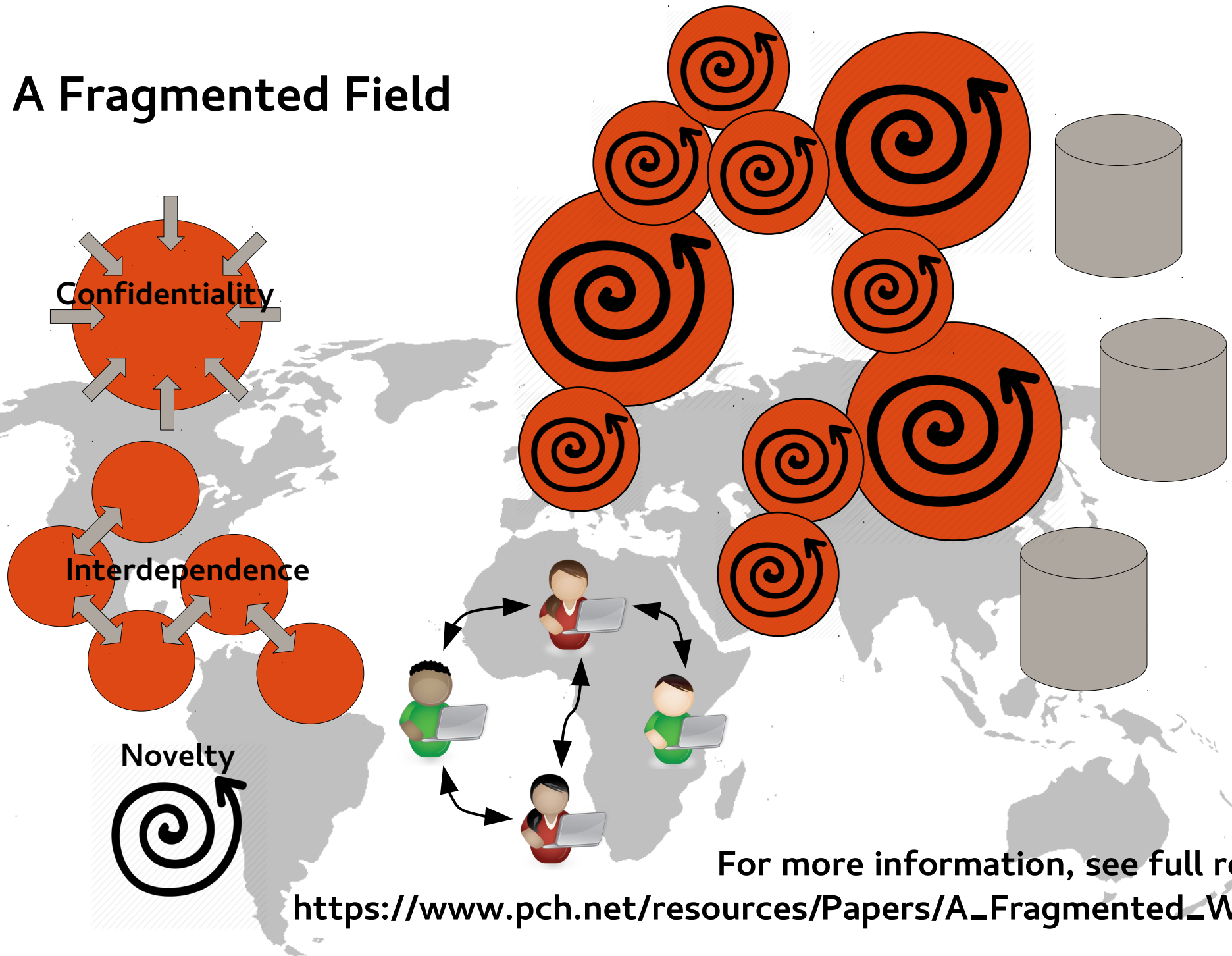
For more information, see full report:
https://www.pch.net/resources/Papers/A_Fragmented_Whole/
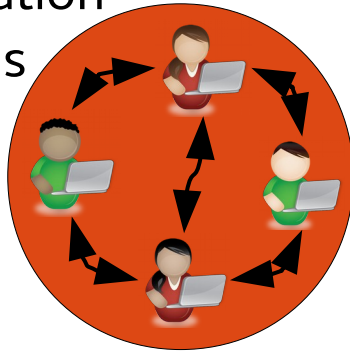
Recommendations

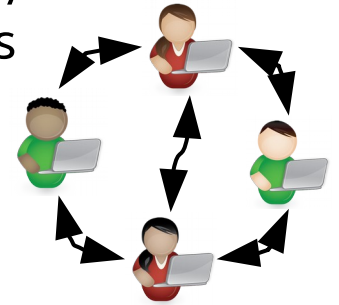Interpersonal relationships as outcomes of institutions
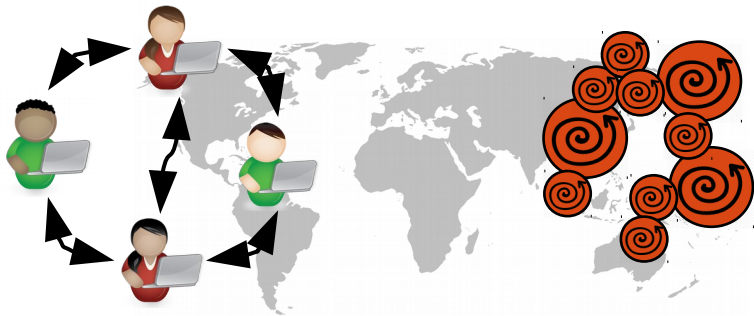
Industry ↔ Education connections

Build training and information sharing into infosec teams

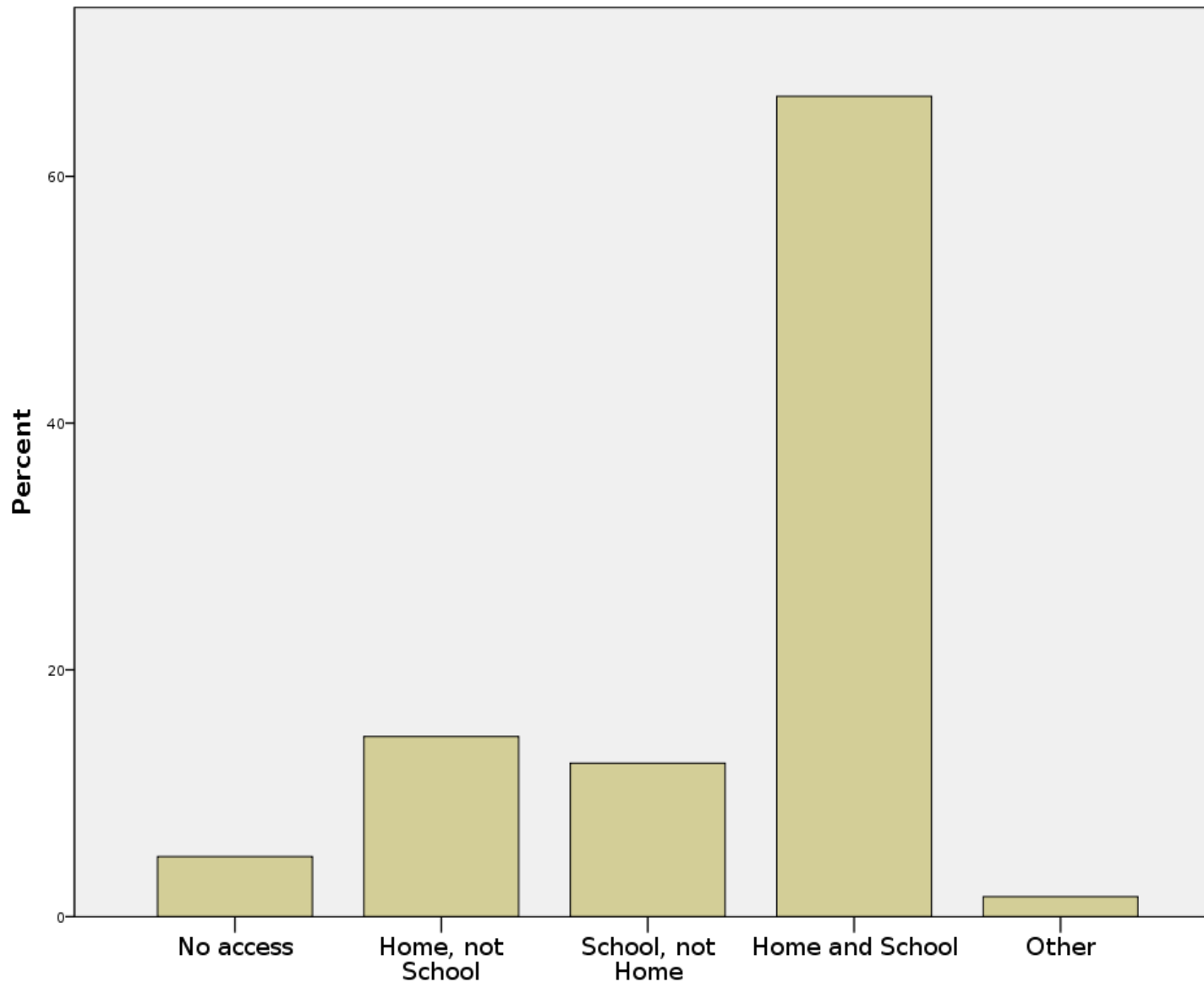General and diversity-focused mentoring programs

Support travel

Support local meetups

Encourage curiosity

Access to computers growing up