INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY
(IC)³

Building a Culture of Information Security

Goal: share practices to create a more cyber resilient organization

With cybersecurity top of mind in many organizations, we will use a session at the (IC)³ annual conference to discuss and share leading practices we have implemented or seen implemented in organization. Our objectives with this session are two-fold:

1. Create an actionable set of practices our members can implement immediately
2. Kick start the next phase of our research on House of Security- understanding some of the issues and practices organizations have used to create a culture of security.

Workshop Outline

Assignment: Prior to the workshop, participants were asked to bring with them an example of a practice or activity their organization has implemented (or they have seen implemented in other organizations) to encourage, teach, and/or create a more cyber secure culture. Some examples:

What is one practice or activity your organization does to build cybersecurity behaviors?

- Phishing emails sent out by the information security team to 'test' staff. If someone opens the attachment or clicks on the link, they are directed to a training module to increase awareness of potential future phishing emails.
- Incoming emails are scanned before being delivered to recipient and if an attachment or link is included, a colorful message is inserted to alert the recipient that this might be a cyber security risk.
- All incoming staff are required to attend a 1-day cybersecurity training program as part of orientation where they are exposed to tricks they may potentially encounter, and appropriate responses they might take to cybersecurity risks.

What to bring to the session: Participants are asked to bring an example (different from the 3 above) from their experience with them. Pick an example that you think is both interesting and different. While we prefer you bring a document or a slide, it is also acceptable to just bring an idea to share with the group in discussion.

Plans for this Conference session: We will break into small groups to discuss examples of cybersecurity practices. Each participant will be given a chance to share a leading practice. The break out groups will then reconvene in the larger classroom to share one or two of the best ideas that emerged from their discussion. We will take notes and create a summary report for (IC)3 members on leading practices shared by the group in addition to creating a more extensive research project to dive deeper into the culture of security.