The Design Group
Design driven by people/organization/society capabilities/needs

• Users are still the weakest link in security
• Systems that are not designed with understanding of human behavior
• Organizations where security is not a top priority
• Incomplete understanding of human, organization, and technology dynamics in socio-technical systems
Users are still the weakest link in security

- Many users don’t have a good understanding of security issues
- Insider threats (well intentioned / malicious)/non-compliance behavior and actions by users
- There is a disconnect between users and IT staff and management (security design that hinders work activities)
- Many users are more focus on getting their job done than security (bypass security procedures, workarounds).
Users are still the weakest link in security

• Why important?
  • Users played a role in the majority of security breaches

• What are barriers?
  • Distrust between IT and users
  • Different objectives in different parties

• Why is progress possible
  • Interdisciplinary groups work together
  • Organizations may be more willing to understand users
Systems that are not designed with understanding of human behavior

• Problems related to password which is a reoccurring significant issue that often leads to data breaches
• The fraud detection systems are not sophisticated enough to incorporate human elements
• Current systems often made the users the weakest link and the users get blame
Organizations where security is not a top priority

• Security investment has not demonstrated effectiveness in reducing data breaches
• Organizations often treat security as an after thought
• Existing security frameworks and policies are not implemented, monitored, and enforced
Incomplete understanding of human, organization, and technology dynamics in socio-technical systems

• Deterrence is frequently used as the primary component in information security policies
• Phishing emails are still successful after extensive exposure and awareness education
• It is still not clear how incentives work in relation to cybersecurity (monetary, spiritual, social good, etc.)