Day 1:

Group 2: Tyler, Jens, Mary, Qing, Ross, Cormac, Rob, Ann

Measurement

- Does cybercrime research focus more on individual or organization behaviors?
- What of important emails and documents blocked by cybersecurity? Costs, etc.
- Since insurance companies sell cybercrime policies to companies, how do they price such policies?
- Since the costs of cybercrime are so poorly understood, what can be done to improve this situation?
- What is the level of cybersecurity at which attackers stop? Can we deter offenders?
- Can we measure cybercrime / security longitudinally even when we don't always have a consistent question to answer?
- "Software on the witness stand"
- How do we measure the reliable security efforts and outcomes?
- How can we assess whether cybersecurity has improved by the next Grand CHallenge in 10 years?

Return on Investment in IT Security???

- If we can't answer this question, CSO has no power to ask for continued support
- CSOs able to get budget without ROI, as boards are scared because of the extent cybersecurity is in the news
- Less that what we ultimately want, since it's hard to quantify
- This is similar to pollution abatement (we want to stay out of the paper for pollution), ut no direct benefit to us
- Society for Risk Assessment: easy to measure costs, hard to measure benefits (particularly indirect)
- Cybersecurity, dealing with an adversary that is strategizing
- Parallels to Environmental Economics

Where is the challenge in measurement?

- The economic value of the effect of cybercrime differs greatly - what are the three most economical categories?
- Where do we expect that we're investing wrongly?
    - How do we differentiate IT spending vs. cybersecurity spending?
        - They are the "same thing" - infrastructure, secure coding, redundancy, etc.
        - How would you allocate the IT spending / cyber across the many dimensions to understand the risks / returns associated with each?
        - Needs to be a clear budget on security, not just IT, even though it's so closely related, need to make sure security is accounted for
        - Have to attach to every IT investment: what does it do to security?
        - Cyberinsurance isn't solving the cyber measurement problem. Data breach disclosure agreements have led to cyber insurance industry
        - Banks can have DDOS insurance, and coverage for fraud
            - Anything that goes beyond data breach, is often not able to be covered

Why wasn't ROI model successful?

How do you measure security, risk, etc. to determine ROI for cybersecurity? There are lots of different theories in different areas. We want to quantify cyber risks, and collect the data that will get us there.

What do we want in a metric? Something I can quantify in my mind, something simple,

- Reputation Loss
    - Stock Price, Lost customers, (Target), qualified earnings drop, man hours to restore,
    - How do you invest in safety (mines)?

What would we want to measure, what is raw data to collect, what would that thing (calculation) be related to

How do we link measures to countermeasures?
Need to end up with effective countermeasures
How do you assign liability if you can't assign negligence?
How do we eliminate crime from humanity...we need to measure it, then look for policies to abate it, eliminating it is impossible

Need to bring everyone in: Put a methodology and RQ's that are carefully worked out

Individual vs. Group

- How do we make CSOs trustworthy?
- Consensus: Can we alliance individual's interests with the organizational goal and security interest?
- Tension: CSos desire to control people vs. desired flexibility
- How do we balance individual and organziational incentives?
- Is there a group between individual and organizational?
- How do we balance the needs of society, organization vs. the needs of the individual?
- How can we improve individual and organizational decision making progress on cyber spaces?
- Understand CSOs perceptions of security and how most users understand security and recommendations for security?

What would be the kind of things we could measure with respect to an individual's security?

Displacement Theory: if I protect my computer, makes integrity better

Organization Focused Thinking as a viable structure: people are consumers doing this in a relationship with companies, and in a corporate context

There's some tension between individual and group interests, but is possible to bridge domains: boundary objects → consensus by increased awareness / education

We're a little bit behind (Upper Eschelon Theory)

Different Levels at which you can take strategic decisions; different incentives, motivations, capabilities

Bridging Measurement and Individuals vs. Groups: Valuable to know people's understanding of their organizations' cybersecurity - is it an impediment or valuable?

People in organizations vs. people as customers of organizations
    Need to understand measurement for this

From organizational perspective, the more data you can collect, the better you can do your job (identifying threats, actors, weaknesses of system) (DROWNING IN DATA)
As employee, would hate for everything to be collected

Employees vs. Sub contractors / Suppliers

Day 2:

Tyler, Jens, Shuyuan, Moury, Cormac, Rob, Ann

Number of times where someone makes a suggestion, and there's an anecdote / example for why it won't work...possibility of finding an answer to solve everything is impossible, so we scope down way too much

Cybercrime statistics bureau, similar to Moury's paper

Would be nice if we could come up with an end goal: cybercrime statistics bureasu where we have done the hard work to identify and collect cybercrime statistics data with good reliability, try to get to quality of traditional crime reporting statistics

- Need to ensure about good reporting (individuals, organizations)
    - Privacy Rights Clearing House (Organizational Data Breaches)
    - IC3 (online fraud)

Cybercrime statistics bureau

- For what question is this the answer?
    - Helps us answer the question on how should we spend marginal dollar?
    - Helps us track progress against cybercrime (or lack thereof) over time
    - Why is this actually better than IC3, Symantec reports, Verizon DBR, FS-ISAC?
        - If we get rank ordering of harms, then we can help prioritize defense (can do CBA properly)
    - Provides accountability to the cybersecurity industry and defenders (CISOs, LE)
    - Increases awareness to cybercrime prevalence and harms, etc.

        - Build a capability to aggressively explore different uses of the data (e.g., consider the value of re-use of US economic statistics)
- Methods of measurement
    - We need mechanisms for reporting
        - Individual victim reporting
        - Organizational victim reporting
        - Improving police reporting?
    - Survey mechanisms
    - Direct measurement
- Measuring harm
    - Ways to quantify harm: financial losses, emotional and physical distress, reputational damage, lost time, number of lost records?
    - Identifying when it is possible to measure harm (card fraud) and when not (bullying)
    - In some cases we need to think of better ways to quantify harm (e.g. for harassment, doxing)
    - In other cases even if we know how to quantify (e.g., ransomware), challenges remain in estimating the aggregated harm
- Measuring defender effort
    - Report man-hours required for investigation, time to detect intrusion, time to remediate intrusion. These are inherently more consistent across victims and feasible to calculate. Can we identify more such measures that can be tracked longitudinally?
- Desirable characteristics
    - Adaptive at picking up trends in attack evolution, where crime originates, which crimes are connected,
    - Actionable: raise awareness, encourage better behavior
    - Rank order of harm impact
- What should the mechanism look like?
    - Who should be reported to and how? Local LE, FBI, online form, Google, phone, live chat bot (clippy for cybercrime victims)?
    - What form should the institution be? Government agency has disadvantages such as slow adaptation, black holes, etc., but they have the key advantage of compulsion under the law (uniform crime reporting act)
        - How can we construct a workable solution that is more agile and can operate without subpoena power.
    - Fold into fbi uniform crime reporting mechanism?
- Challenges
    - Underreporting by individuals
    - Underreporting by firms
        - Absent compulsion, how can we incentivize firms to share information on incidents? What are acceptable terms?

        - Normalizing definitions of cybercrime categories [can we come up with durable categories that don't change every n years]
        - Normalizing what counts as an incident
        - Normalizing what constitutes becoming a victim
            - Does experiencing credit card fraud but not losing $ count as a victim? Some would-be victims say yes, others say no
        - How to incentivize reporting?
            - Individual case files to give personalized feedback on progress, relevant information to your experience (what is being done in general, how to protect for the future)
            - Develop dynamic feedback to show the value in reporting.
            - Leverage existing collection efforts by firms
- Needs
    - Define cybercrime categories, and how it maps to the data we'd like to collect and the appropriate mechanisms
    - Well-trained social science staff to instrument surveys, understand data issues, design and apply methodologies
    - Data scientists to analyze data
    - Well-trained computer scientists to collect data on crimes, to identify trends
    - Visible

Existing efforts

- IC3: primarily self-reported financially motivated cybercrimes
- PRC: data breaches
- FBI press releases on business email compromise
- FTC reporting mechanism on identity theft
- Stopbullying.gov says report to local police
- NW3C

Problem? This is decentralized

Goal: rank order list of cybercrime harm (in terms of dollar amount)

Suggestions for specific people

- FBI data scientists (Rob Axtell knows them)
- Criminologists with awareness to crime statistics reporting
- Cybercrime measurement researchers
- Physical crime statistics experts (e.g., academics who use NCVS, UCR)
- HCI/UXI researchers (for improving reporting mechanism)
- Organizational behavior researchers (for incentives of orgs/firms to report cybercrime)
- Policy economists/econometricians who do cost-benefit analysis
- Data archivists (IS people who know about categorization, etc.)