WHY IS CYBERSECURITY HARD?

Cybersecurity is not just a technical problem

Cyberspace is governed by a different set of rules

Cybersecurity is “new” and we’re still learning

Cybersecurity is also an economic, psychological, and human behavioral challenge, all rolled into one

The concepts of distance, borders, and proximity all operate differently in cyberspace compared to the physical world

We haven’t had the time or the experience to develop the comprehensive frameworks required to address cyber risk
SETTING THE STAGE: ACTORS & TRENDS

The four primary types of cyber adversaries
- Hactivists: Act in support of a cause
- Terrorists: Leverage cyberspace to recruit
- Criminal Organizations: Profit off malicious activity
- Nation States: Pursue their national interests

More broad
The attack surface is exponentially increasing

More frequent
Volume of malicious cyber activity is increasing

More dangerous
Actors are increasingly moving to more destructive activity

More disruptive
Potential impacts of a cyber incident are increasing

Volume and diversity of connected devices increases complexity

Low barriers to entry and high ROI incentive actors

Critical infrastructure is at the center of actors’ malicious activity

Digital dependence is making society increasingly vulnerable

Because of these actors, the cyber threat is becoming....
BUT, IT’S NOT ALL BAD

All malicious actors face constraints:

> Hollywood ≠ real life
> Collateral damage uncertainty
> Capacity limits
> Limited freedom of action

Nation states face some additional constraints:

> Intelligence dilemma
> Third country conundrum
> Integration requirements
TAKE ACTION: BUILD YOUR CYBER TOOL BOX

C-Suite Time & Attention
Focus executives’ time and attention on cyber issues

A holistic risk-management framework

Communication

Performance Metrics
Adopt some metrics, measure them, and adjust over time

Incident Response Plan
Develop an IR plan, then practice/perfect before an incident

Accountability
Shift the culture by setting expectations and creating incentives

External expertise

Information sharing organizations (e.g. ISAC/ISAO)

Relationships w/law enforcement & network defenders
QUESTIONS?