LEVELING UP: HOW SHARING THREAT INTELLIGENCE MAKES YOU MORE COMPETITIVE

CYBER THREAT ALLIANCE

Michael Daniel
President & CEO

WHAT DO WE MEAN BY INFORMATION OR THREAT SHARING?

Different kinds of sharing serve different purposes:

- Technical data
- Context
- Attribution
- Best practices
- Defensive measures and mitigations
- Strategic warning
- Tactical warning
- Situational Awareness

We often act as if all organizations can share all of these information types all of the time – but that's not true.

WHAT HINDERS THREAT SHARING?

Volume and diversity of information poses a problem

Hard to directly measure the ROI on sharing

Technical
Need an accepted standard and ability to separate signal from noise

Business
Need to show a benefit to sharing

Four factors constrain threat sharing:

Legal
Need clear frameworks on what is permissible

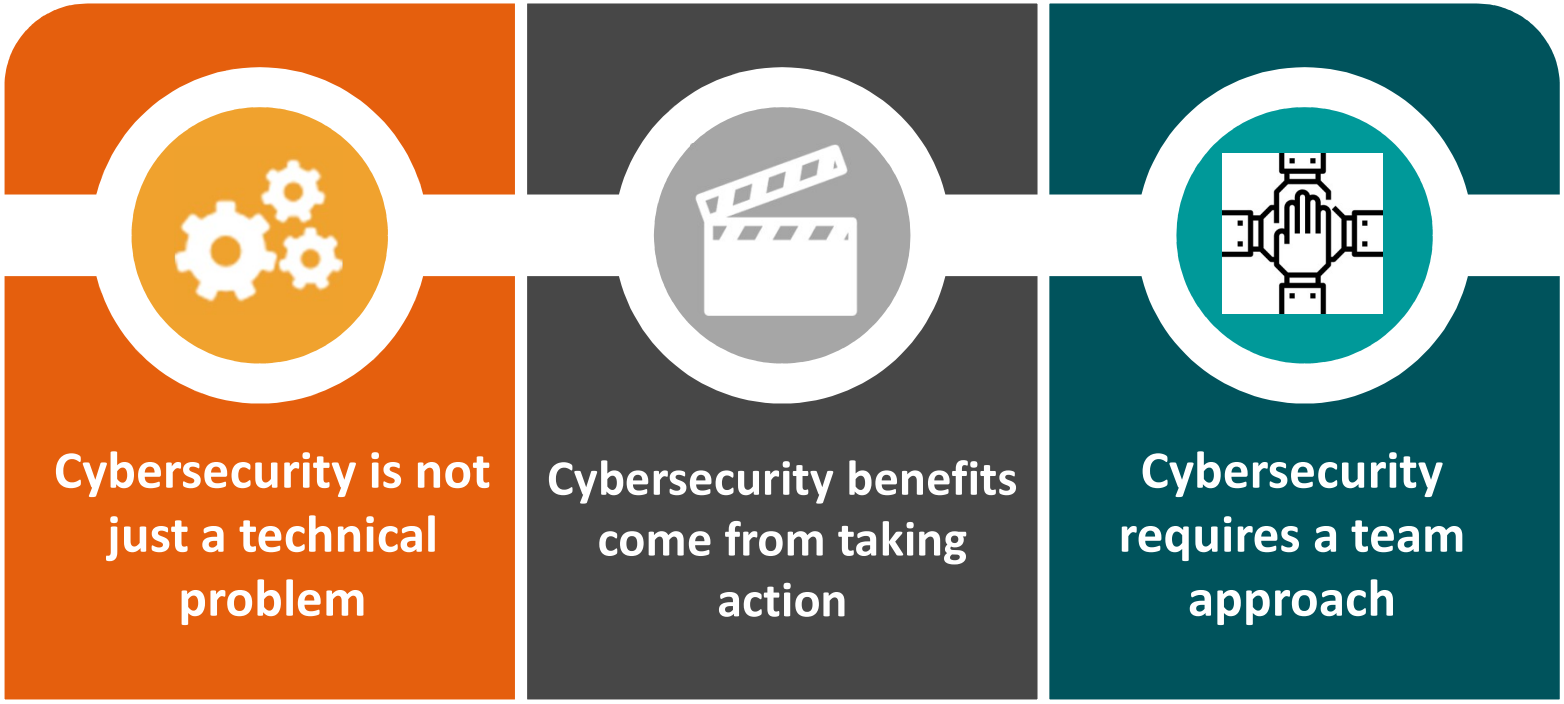
Cultural
Need to change how competitive advantage is perceived

Anti-trust, privacy, GDPR, and other parameters can be unclear

We have to know more than the other guy for people to buy our stuff

CYBER THREAT ALLIANCE

WHY DOES THREAT SHARING ENHANCE YOUR COMPETITIVE EDGE?



Cybersecurity is also an economic, psychological, and human behavioral challenge; no organization has expertise in all these areas.

It's not what you know, but what you do with what you know.

We need to consider comparative advantage.

CYBER THREAT ALLIANCE

THREAT SHARING EXAMPLES FROM CTA: LEVELING UP IN THE SHARING GAME

WannaCry threat sharing reduced the "fog of war"

We got to the right answer much more quickly

VPNFilter threat sharing amplified our actions

Coordinated protections boosted impact

Automated sharing enhanced outputs

All our members received information that was new to them

CYBER THREAT ALLIANCE

OKAY, WE'RE SHARING. SO NOW WHAT?

- Build up sharing organizations
  - Focus technical sharing efforts on technically capable entities
  - Allow companies to share according to their comparative advantage

- Enable more robust sharing between sectors
  - Spread lessons learned across sectors
  - Create regular, cross-sector links

- Translate sharing into action
  - Use shared data to create outputs that systemically disrupt adversaries
  - Employ shared data to identify specific actions that different parts of the ecosystem should take

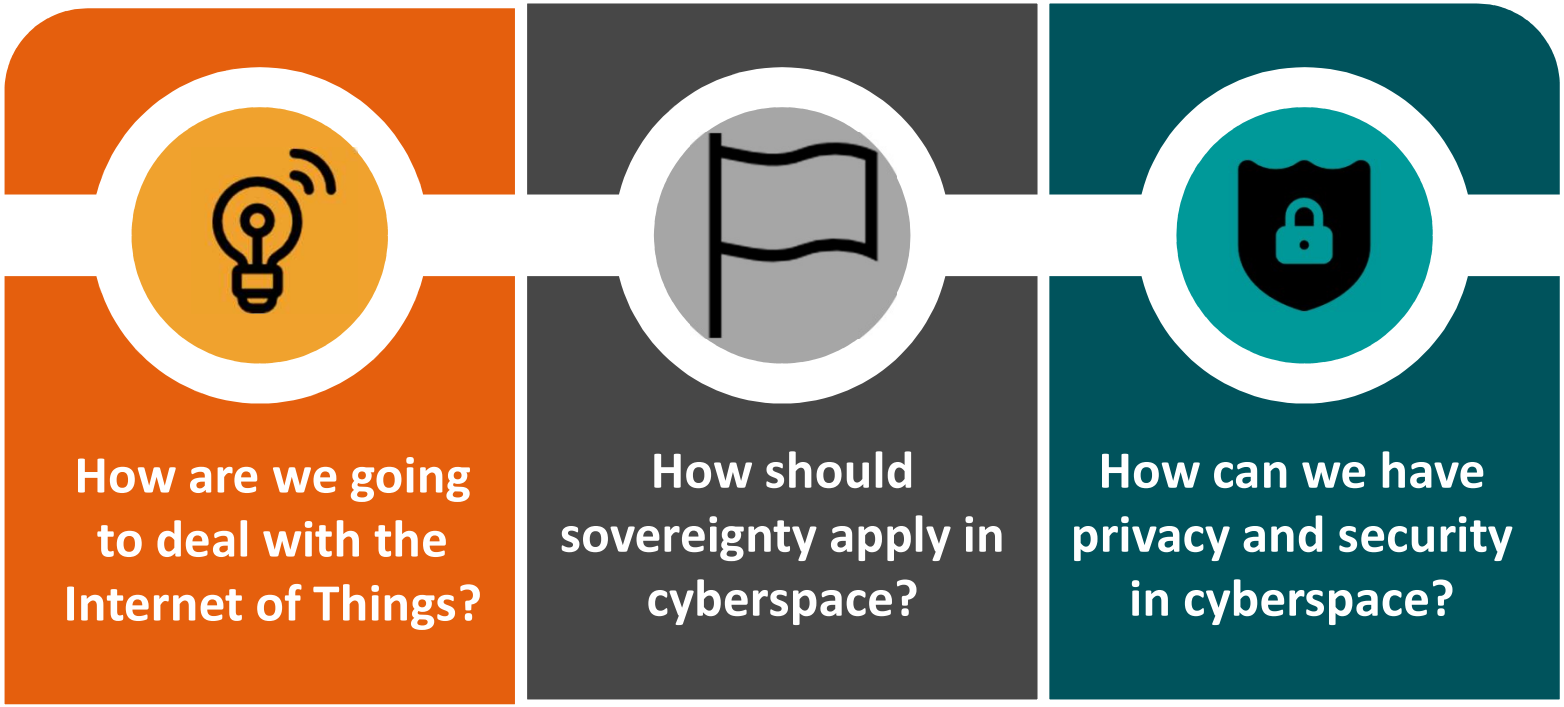
CYBER THREAT ALLIANCE

QUESTIONS?

CYBER THREAT ALLIANCE

BACKUP SLIDES

WHAT ARE SOME KEY ISSUES DRIVING GLOBAL CYBERSECURITY POLICY?



Once connected devices can kill people, regulation is inevitable.

We need new tools to manage friction in cyberspace.

Privacy and security should reinforce each other, but can be mutually destructive.

CYBER THREAT ALLIANCE

TAKE ACTION INTERNALLY: BUILD A CYBER TOOL BOX

Each element depends on the others to be effective

CYBER THREAT ALLIANCE

TAKE ACTION EXTERNALLY: DON'T GO IT ALONE

Organizations must reach across boundaries and engage with external actors

CYBER THREAT ALLIANCE

NATION-STATE CYBER CAPABILITIES: BENEFITS, CONSTRAINTS, AND RISKS

Benefits

- Effective
- Relatively cheap and fast
- Levels the playing field
- Deniability

Constraints

- Intelligence dilemma
- Third country conundrum
- Bureaucratic challenges
- Collateral damage uncertainty
- Tool reuse

Systemic Risks

- Attribution difficulties
- Offense favored over defense
- Unintended consequences

CYBER THREAT ALLIANCE

NATION-STATE CYBER CAPABILITIES: DEALING WITH THE SYSTEMIC RISK

Analogies that don't apply:

Border security

Missile defense

Nuclear deterrence

Approaches having some promise:

Operational Collaboration

Transparency

International Norms

Confidence-building measures

Resilience

CYBER THREAT ALLIANCE