Preparing the Village –
Lessons Learned in Cross-Industry Vulnerability Disclosure

Phillip Misner,
President – Industry Consortium for the Advancement of Security on the Internet (ICASI)
Principal Security Group Manager, Microsoft Corporation
@phillip_misner

The PSIRT Rhythm

Vulnerability reported

Triage

Fix

Release

Acknowledge

Vulnerability reported

Triage

Fix

Release

Logo/Branded Website

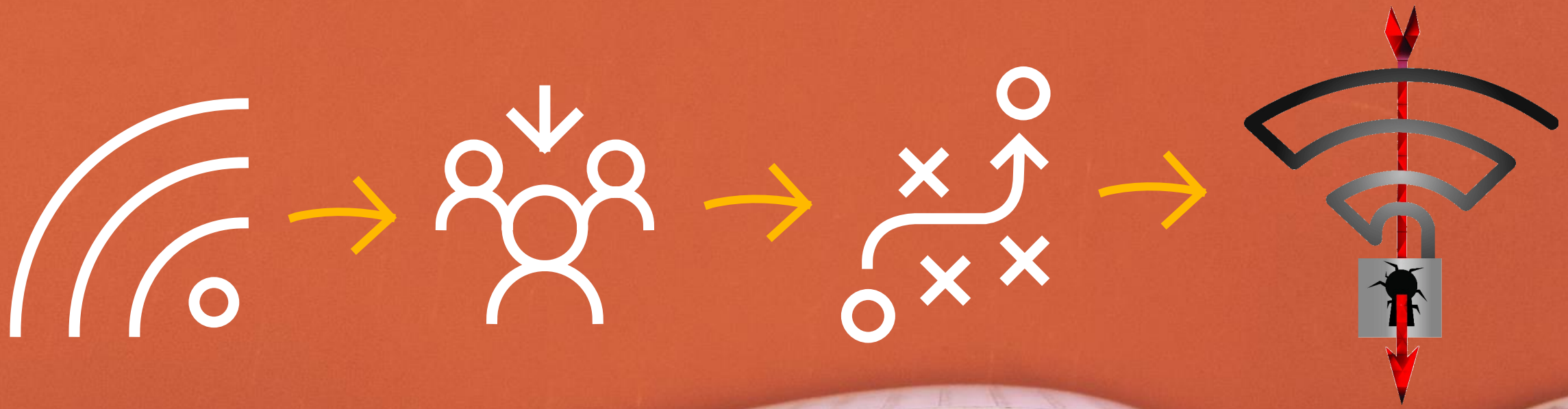
Acknowledge

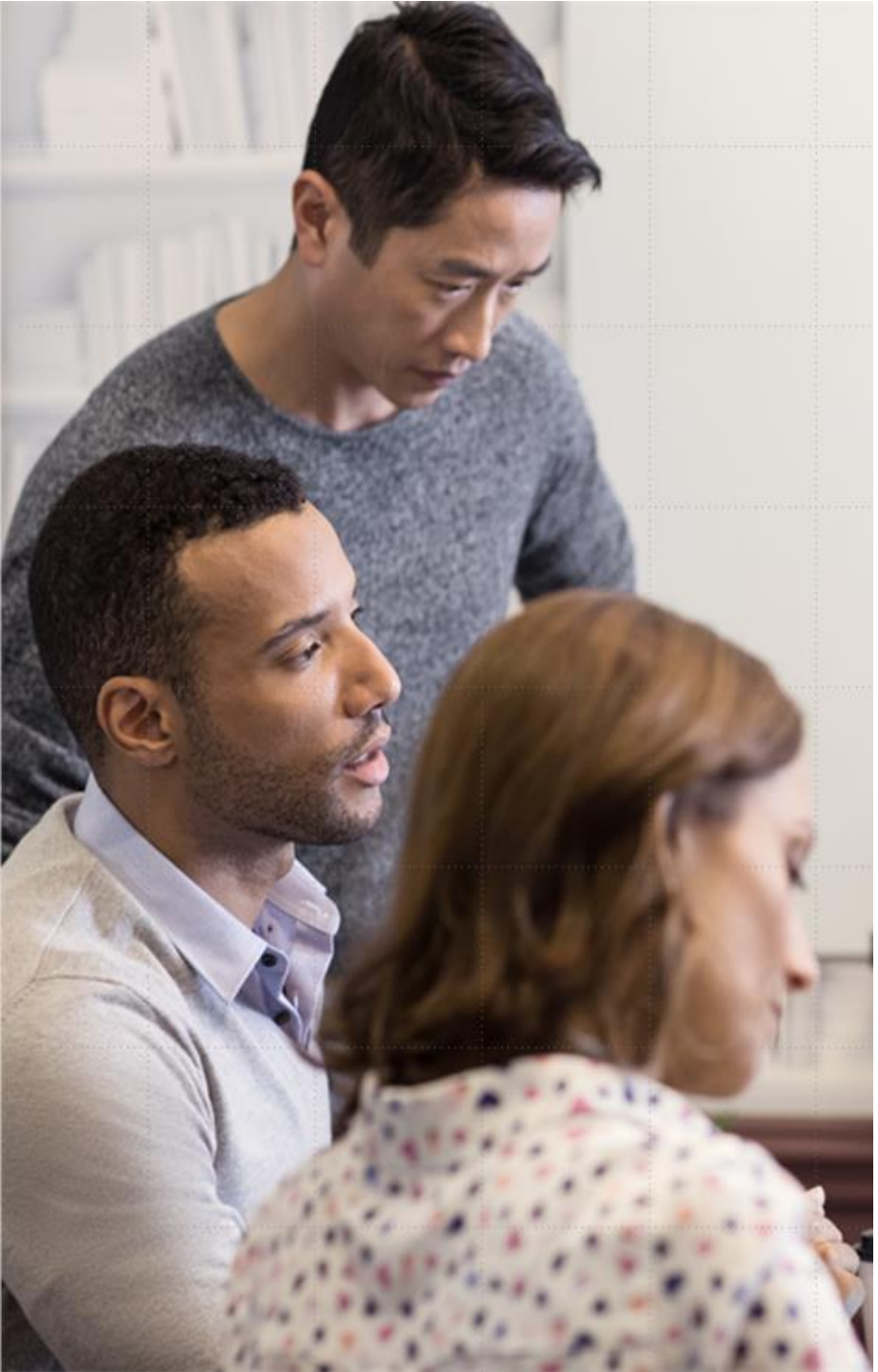
Vulnerability reported

Triage

Wait! World error.

Our story begins…





Industry Consortium for the Advancement of Security on the Internet (ICASI)

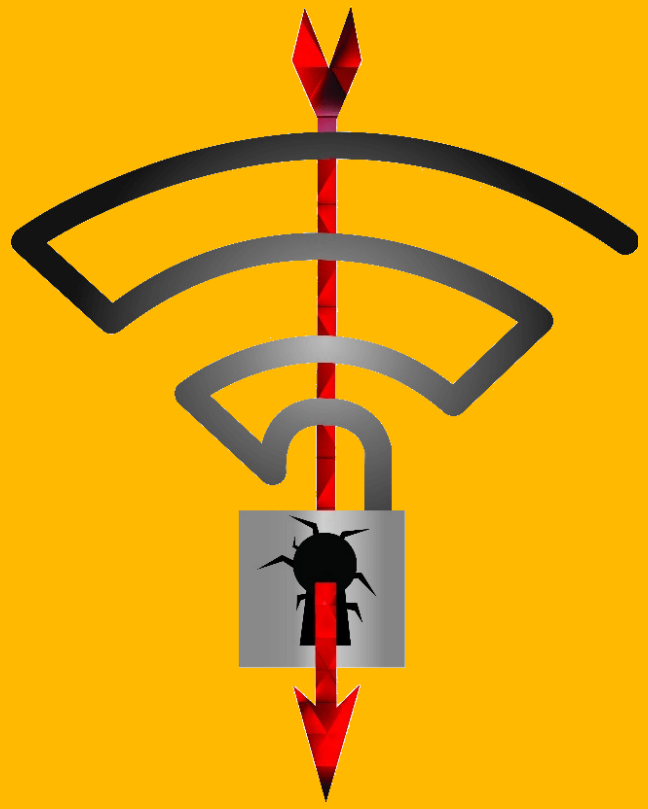
- Made up of 11 industry members (Cisco, IBM, Intel, Juniper Networks, Microsoft, A10 Networks, Amazon, Blackberry, Honeywell International, Oracle, & VMWare)

- Working together to drive security, implement strategic solutions, and enhance the global security ecosystem.

- Developing & sharing best practices
- Collaborate on ecosystem wide problems and awareness
- Multi-party Vulnerability Disclosure process (USIRP)

- https://www.icasi.org

icasi™



Our role in KRAck

- ICASI played the role of industry coordinator
- Using our pre-established trust network and tested incident response process we brought in industry players that could directly address the vulnerabilities
  - Consolidated and gave forum to the researcher to address major industry PSIRTs at once
  - Utilized trust network between members to share understanding and possible solutions to the report
  - Utilized light-weight NDA to bring in other industry members that were not part of the consortium (8 in total)
- Engaged with the researcher affinity groups to broaden reach to affected PSIRTs
  - CERT/CC
  - WiFi Alliance
- Orchestrated single landing page for industry response to KRAck vulnerabilities

/things we learned

Things we all struggle with

1. Trust at scale
2. Asset Management
3. Understanding dependencies

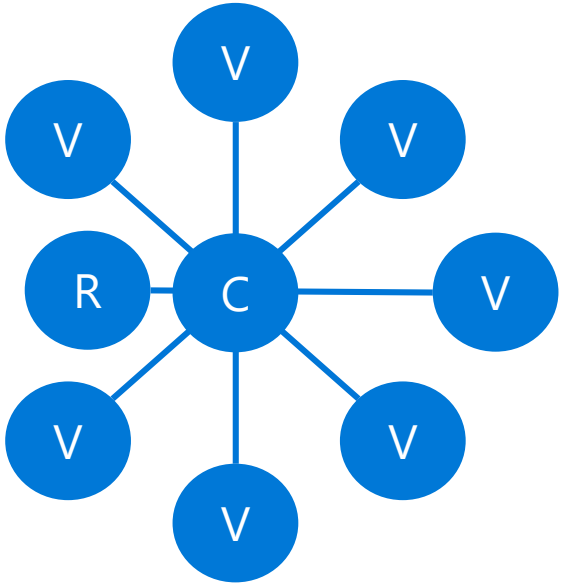
What Challenged Us

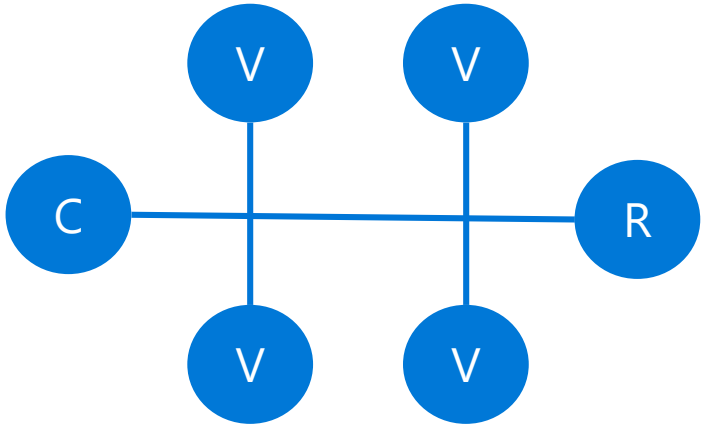
- Secure communications
- Bringing new people up to speed
- Rapidly deploying knowledge after release

What Went Well

- Collaborative trust structure
- Quick way to establish trust
- Coordination with researcher and each other on messaging
- Partnering with other affinity groups

Multi-party Vulnerability Disclosure



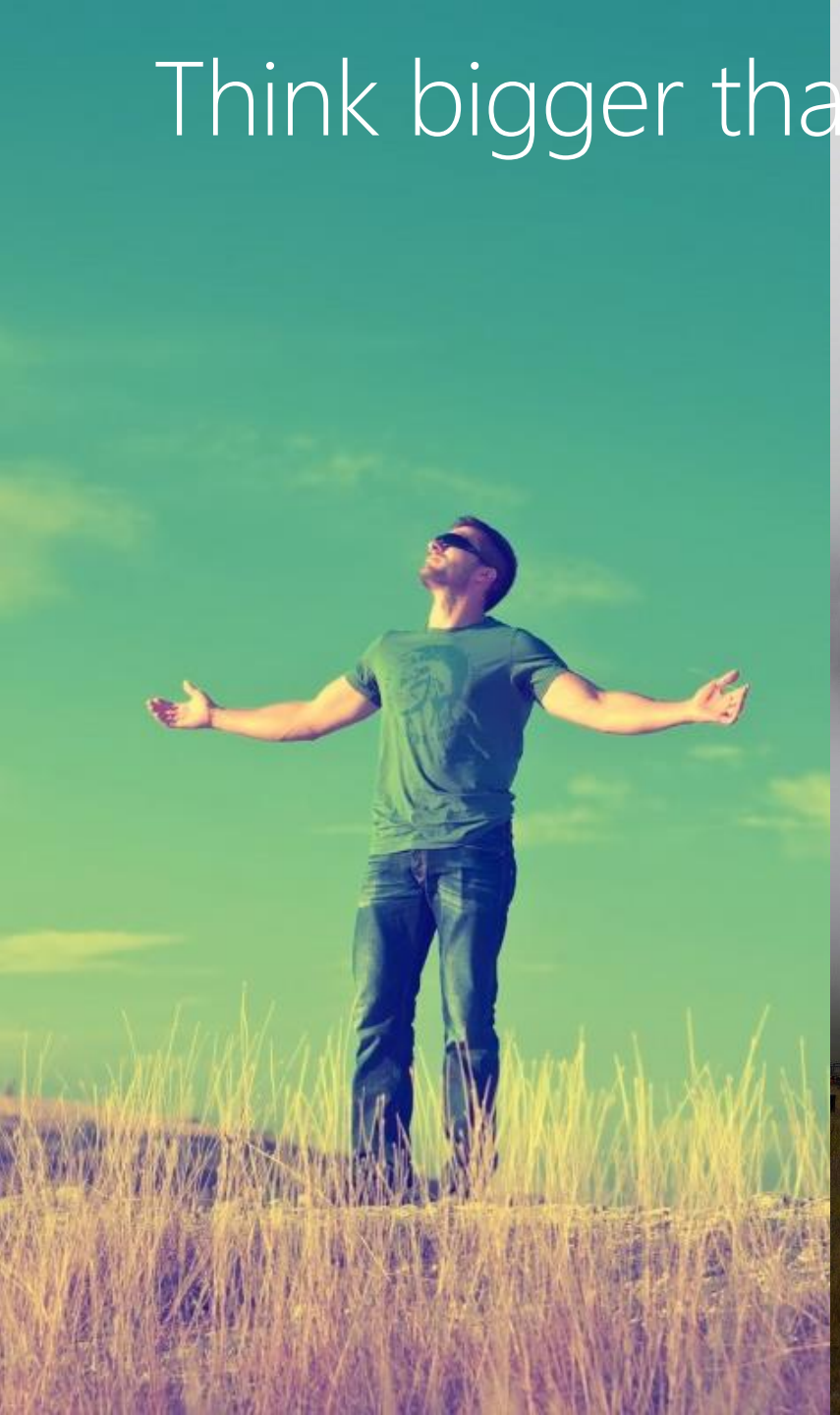


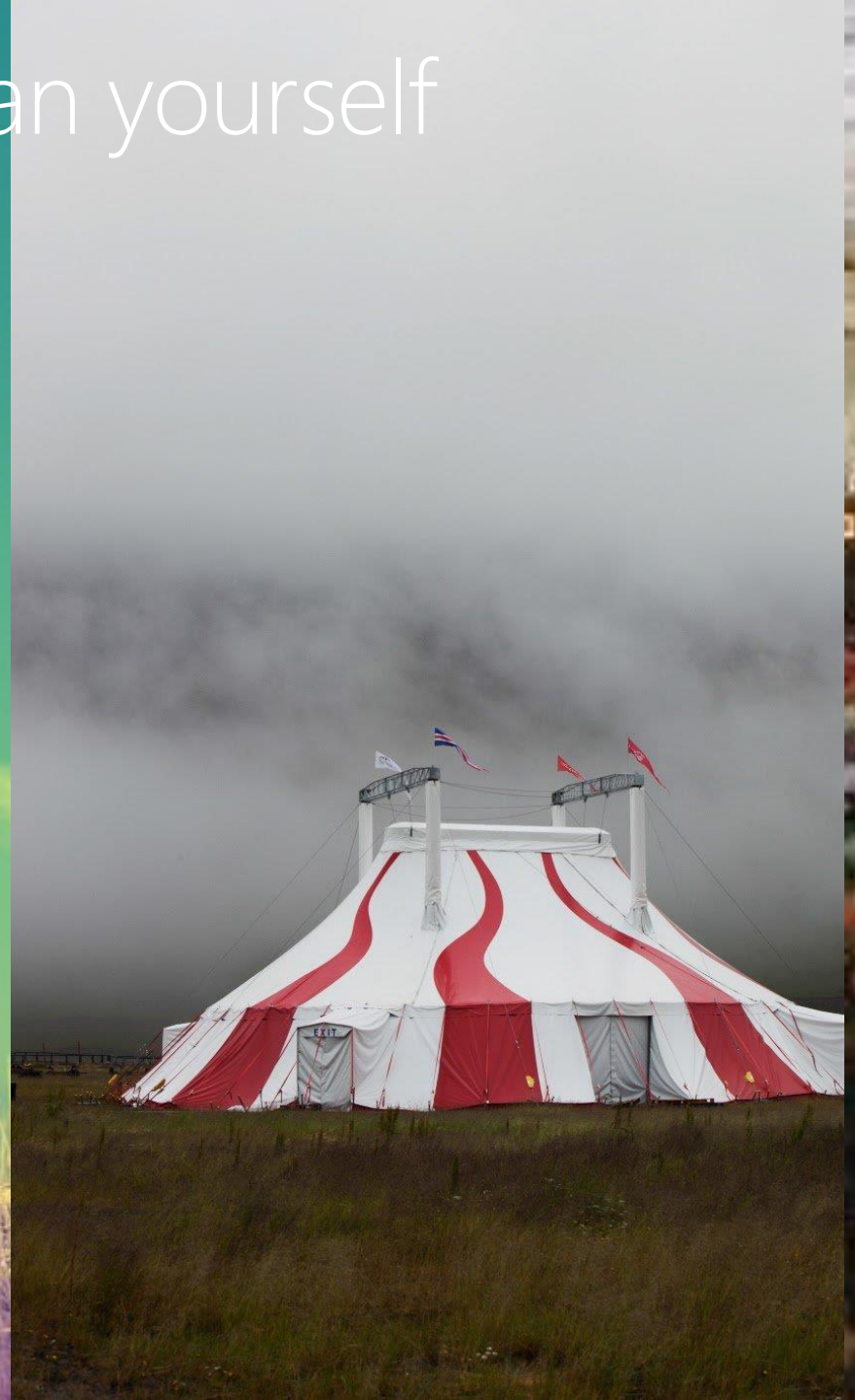
1. Trust
2. Collaboration
3. Focus on the outcome

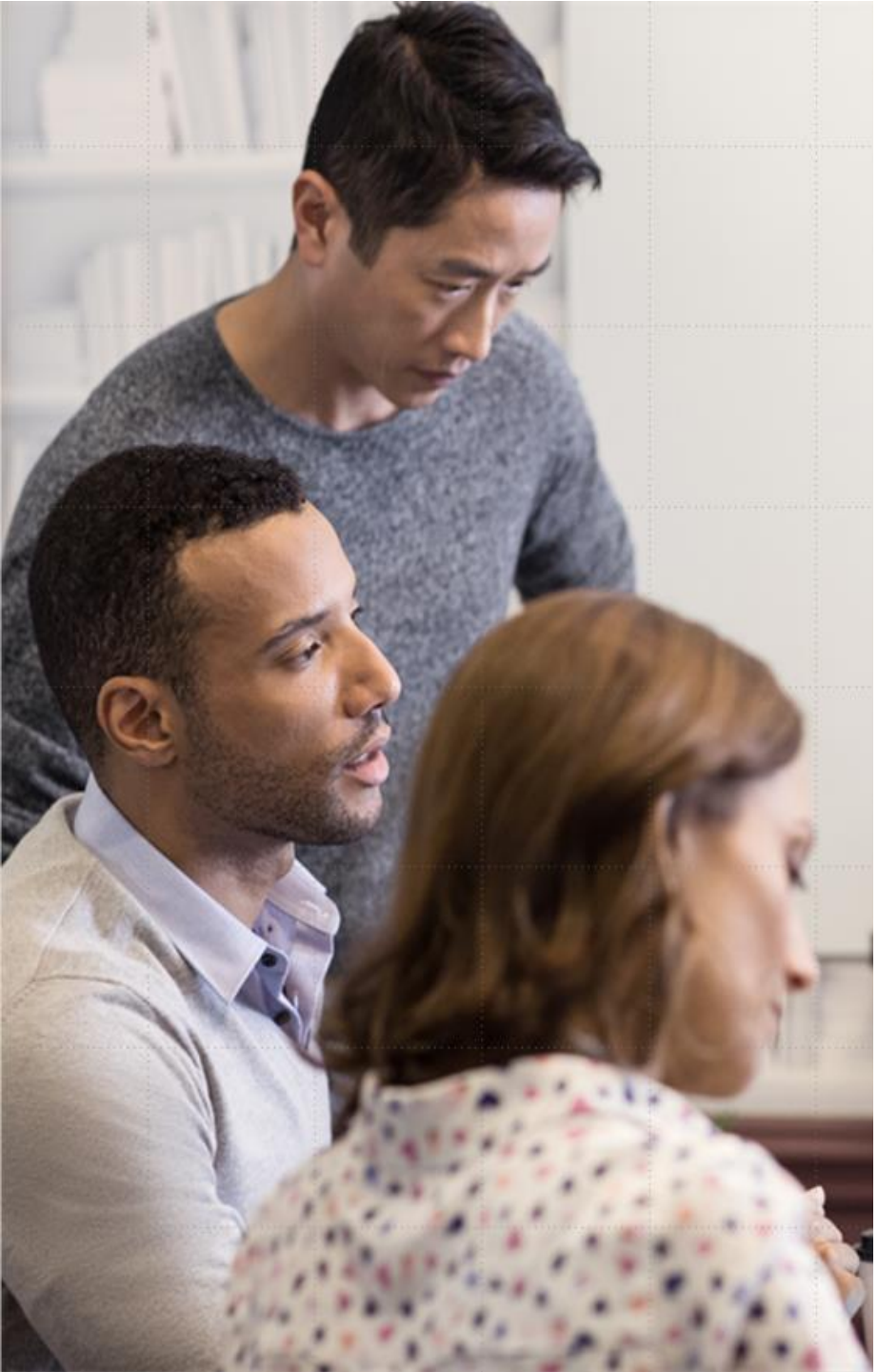
Lessons to Better Fix & Disclose

1. Think bigger than self
2. Trust relationships
3. Tents
4. How to share
5. Create Orchestrator Role
6. Parachute cords
7. Softer landing

Think bigger than yourself







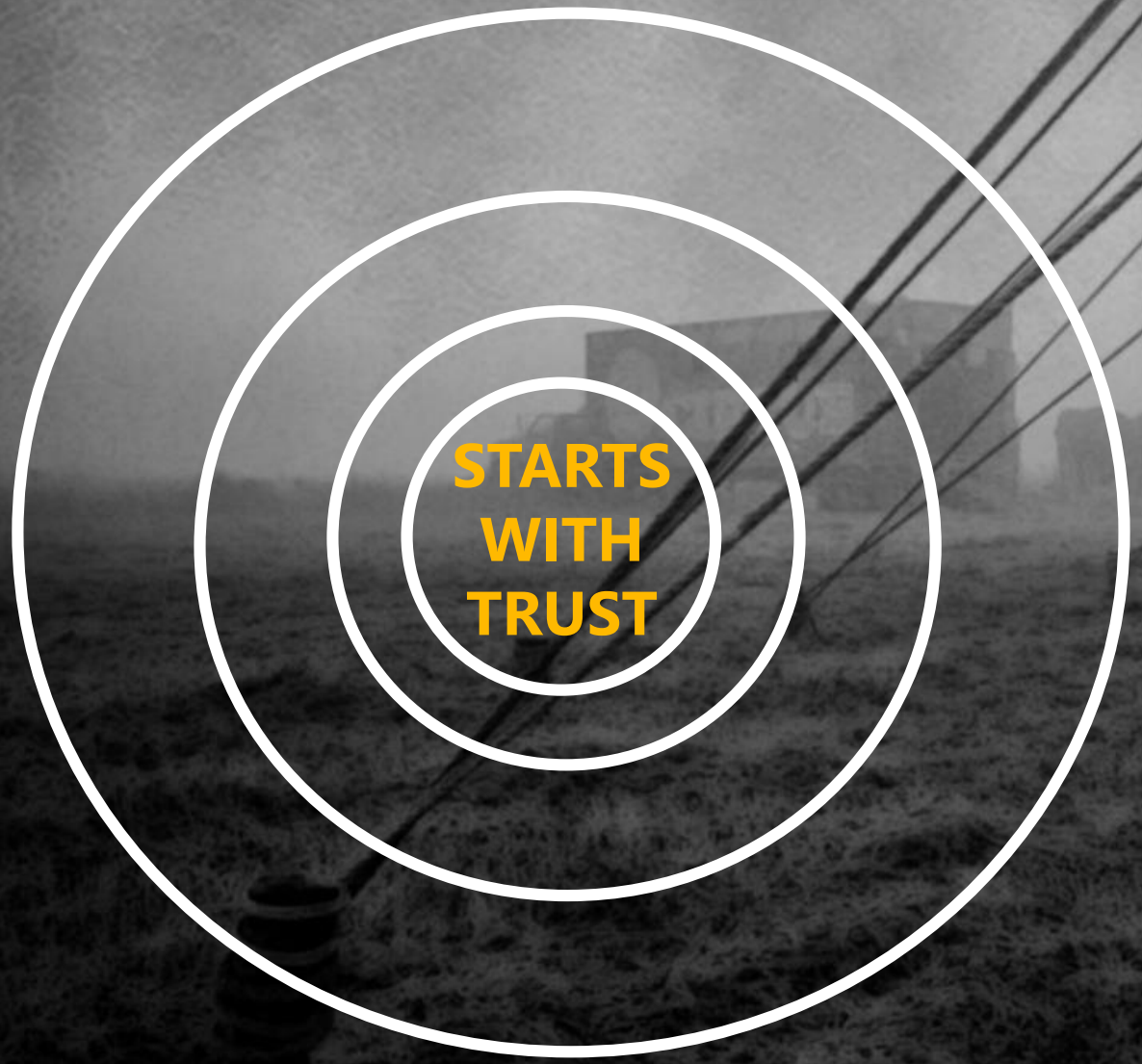
Trust relationships

- How do we trust and scale for this challenge?
- Shared goal to protect the ecosystem

- Likely means multiple trusted communities
- Need to be built before incidents

- Trust is absolutely central to succeeding with Multi-party Vulnerability Disclosure

Tenting



- Fix Providers
- Enablers
- Affinity Groups or Scalers
- More?

- When does each tent engage?

How to share?

- PSIRTs have tackled this problem within organizations?
- Often based on least privilege
- Tied closely with engineering processes

- How do we turn this outward?
- What are the artifacts that need to be shared?
- Executive & Legal review may be required

- Danger of just consuming…

Create an orchestrator role

- Dedicated role
- Empowered and recognized by all participants
- Contact conduit with researcher
- Balancer of competing priorities

Parachute cords

- What are your triggers for action?

- Critical safety measure (operational risk management)
- Often thought of too late or not at all

- Scenarios are often durable
- Discuss and agree prior to incidents

Softer landing

- What happens at release?

- By definition, tent will limit participants.
- How do you bring community up to speed?
- How do you avoid enabling attackers?

- Greatest area we can improve and see big gains

The Work Ahead

Our Remaining Work as a Community

- Define and refine the community norms
- Develop communities of trust
- Create a better soft landing
- What is the role of government CERTs in this and when should they be notified?

Some Opportunities

- FIRST's Vulnerability Coordination SIG
- FIRST's Vendor SIG
- Trusted Communities like ICASI

Thank you

phillipm@microsoft.com
@phillip_misner