RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AIR-F03**

How sharing threat intelligence hones your competitive edge

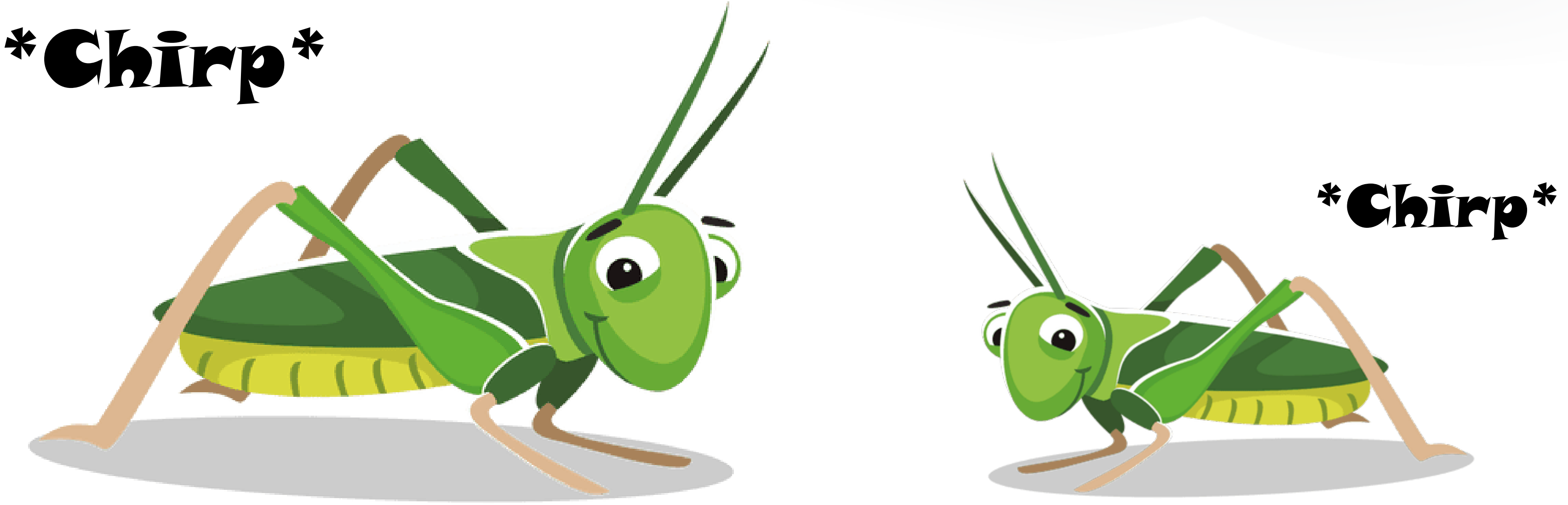
Michael Daniel

President & CEO
Cyber Threat Alliance
@CyAlliancePrez

Typical reasons given for why cyber companies should share threat intelligence…

- It’s for the greater good
- It’s the solution for our cybersecurity problems
- The bad guys do it all the time, so the good guys should too
- Sharing is caring

What usually happens in reality:

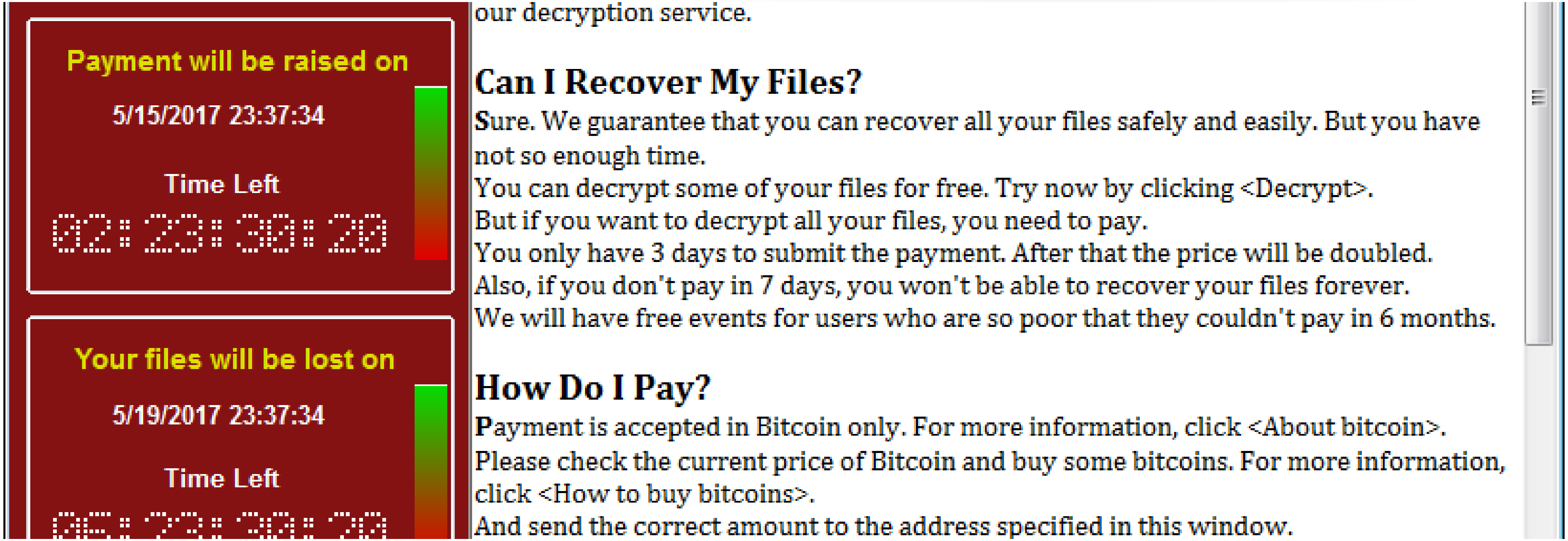


IT TURNS OUT THREAT SHARING IS EASY TO TALK ABOUT, BUT HARD TO DO

Even harder to do consistently at high quality and large scale

Really, really hard in the face of competitive pressures

It’s makes you WannaCry….



Payment will be raised on

5/15/2017 23:37:34

Time Left

02:23:30:20

Your files will be lost on

5/19/2017 23:37:34

Time Left

06:23:30:20

our decryption service.

Can I Recover My Files?

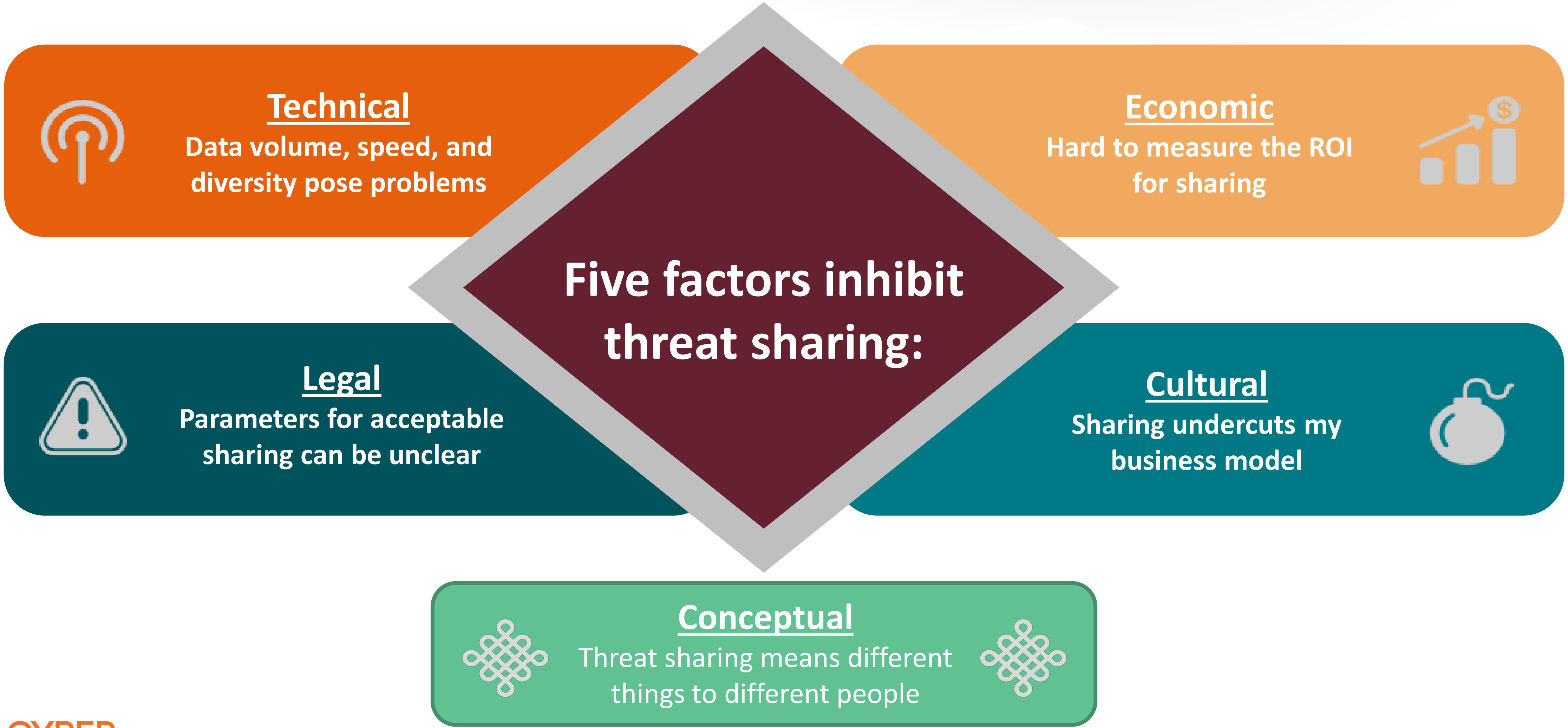
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.

CTA’S SHARING ACTIVITIES AROUND WANNACRY MADE THE ENTIRE INDUSTRY BETTER OFF, BUT ALSO DIRECTLY HELPED OUR MEMBERS

What makes threat sharing so hard?



Five factors inhibit threat sharing:

Technical
Data volume, speed, and diversity pose problems

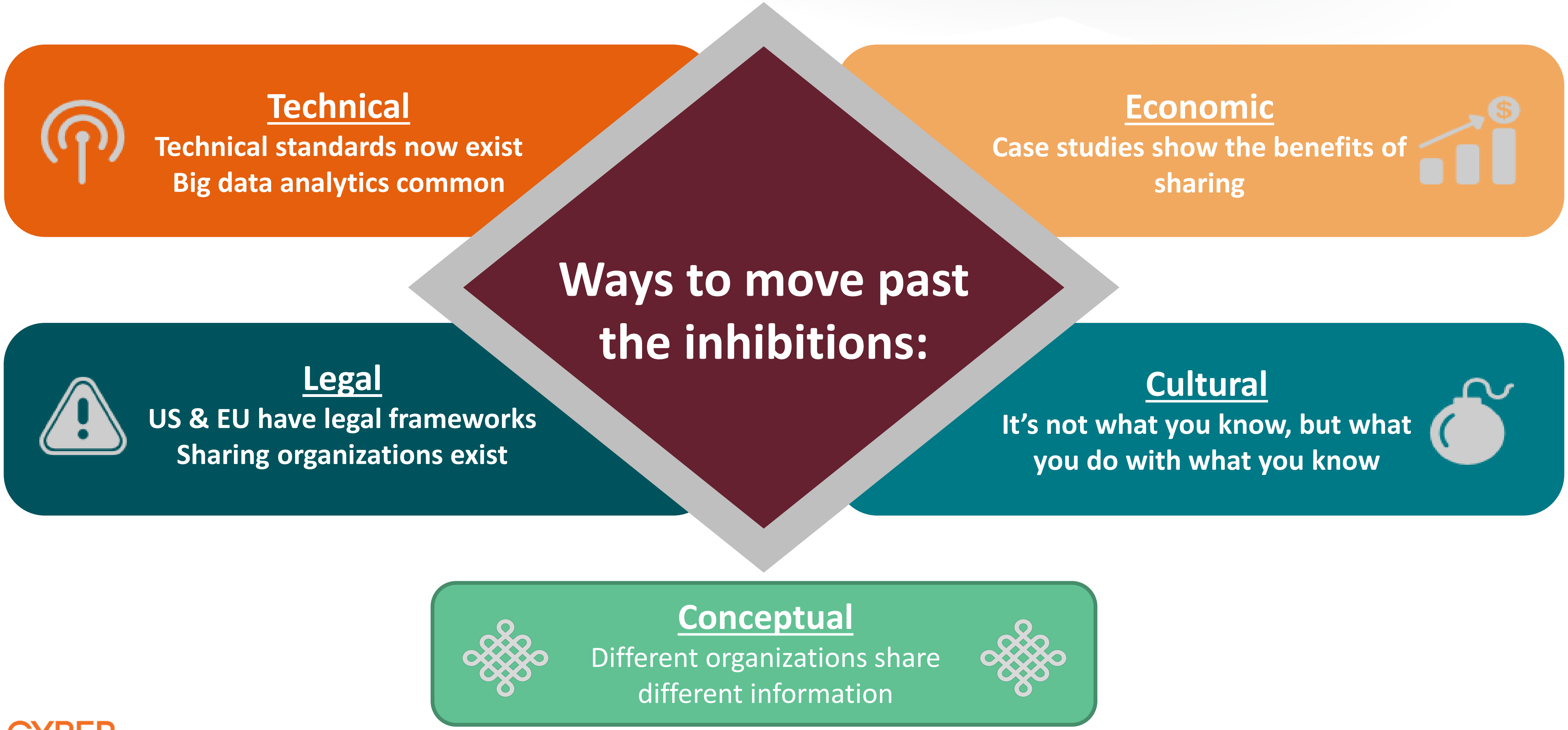
Economic
Hard to measure the ROI for sharing

Legal
Parameters for acceptable sharing can be unclear

Cultural
Sharing undercuts my business model

Conceptual
Threat sharing means different things to different people

But we can overcome these barriers



Ways to move past the inhibitions:

Technical
Technical standards now exist
Big data analytics common

Economic
Case studies show the benefits of sharing

Legal
US & EU have legal frameworks
Sharing organizations exist

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

Conceptual
Different organizations share different information

Beyond beneficial: threat sharing makes you better as a company

How Does Threat Sharing Enhance Your Competitive Edge?

Cybersecurity is not just a technical problem

No organization has expertise in all the facets of cybersecurity.

Increased security comes from taking action

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

End-users are demanding a team approach

Comparative advantage should drive what organizations do.

How Does Threat Sharing Enhance Your Competitive Edge?

No single company sees all malicious activity

Every organization can learn something from sharing.

Regular sharing generates connections and ideas

Sharing forces you to defend your conclusions.

Exchanging business cards in a crisis is a bad idea

It builds the connections needed to deal with crises.

Honing your threat sharing skills

Effective threat sharing requires answering three questions:

- ❑ Who is sharing?
- ❑ What information are they sharing?
- ❑ What purpose are they sharing it for?

The answers to these questions enable you to derive and identify the value you receive from sharing by:

- ➢ Focusing on relevant information
- ➢ Aligning sharing goals with business needs
- ➢ Tracking useful metrics to improve performance over time

Focusing your sharing efforts

Eight types of relevant information:

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

Five types of organizations:

1. Cybersecurity providers, platform providers, ISPs
2. Information sharing organizations
3. Large companies and organizations
4. National government agencies
5. Local government agencies, small and medium businesses, and individuals

RSAConference2020

Case Studies & Lessons Learned from the Cyber Threat Alliance

Threat Sharing Examples from CTA

Automated sharing enhances outputs

All our members receive information that was new to them

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

Threat Sharing Examples from CTA

Early sharing fill in gaps and enhance defenses

Our members can put protections in place ahead of public release

Working Groups focus threat sharing on particular events or threats

We can use shared information to better disrupt malicious activity

Bluekeep threat sharing sped up defensive measures

Customers were protected more quickly

Lessons from our sharing experience

- **Something is better than nothing**
  - Do not have to share everything for sharing to be useful
- **Automation is important for technical sharing**
  - Need speed and scale
- **Humans are important too**
  - People have to do something with the information
- **Sharing is hard work**
  - The technical parts are difficult, but the non-technical parts are more difficult

Applying these lessons in the real world

Applying these lessons at the organizational level

- **If your organization produces, collects, or provides threat intelligence:**
  - Analyze what you can share and what you could benefit from receiving
  - Join a formal threat sharing organization
  - Automate the technical intelligence sharing
- **If your organization consumes threat intelligence:**
  - Ask your vendors how they share threat intelligence across the industry
  - Ask your vendors to validate the intelligence they share with you
  - Make threat sharing an evaluation criterion in your cybersecurity contracts

Applying these lessons at the organizational level

- **If your organization shares threat intelligence amongst members:**
  - Update your business rules to encourage sharing
  - Focus on information types that fit your comparative advantage
  - Build relationships with other threat sharing organizations across sectors and geographic regions
- **If your organization is a national government agency:**
  - Articulate priorities clearly
  - Focus sharing with the private sector on your comparative advantage (hint: it’s <u>not</u> technical data)
  - Encourage cross-sector and international sharing

Applying these lessons across the ecosystem

- **Translate sharing into action**
  - Identify specific actions for different parts of the ecosystem to take
  - Identify real/perceived barriers to action
  - Collaborate to systemically disrupt adversaries
- **Ensure policy and law supports sharing and collaboration activities**
  - Eliminate real or perceived barriers to sharing and collaboration
  - Create positive incentives for sharing and collaboration
  - Mitigate unintended consequences