RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Disrupting the Progression of a Cyber Attack

SESSION ID: HT-R04A

Brian Honan

Chief Executive Officer
BH Consulting and IRISSCERT
@BrianHonan

Dwayne Melancon

Chief Technology Officer
Tripwire
@ThatDwayne

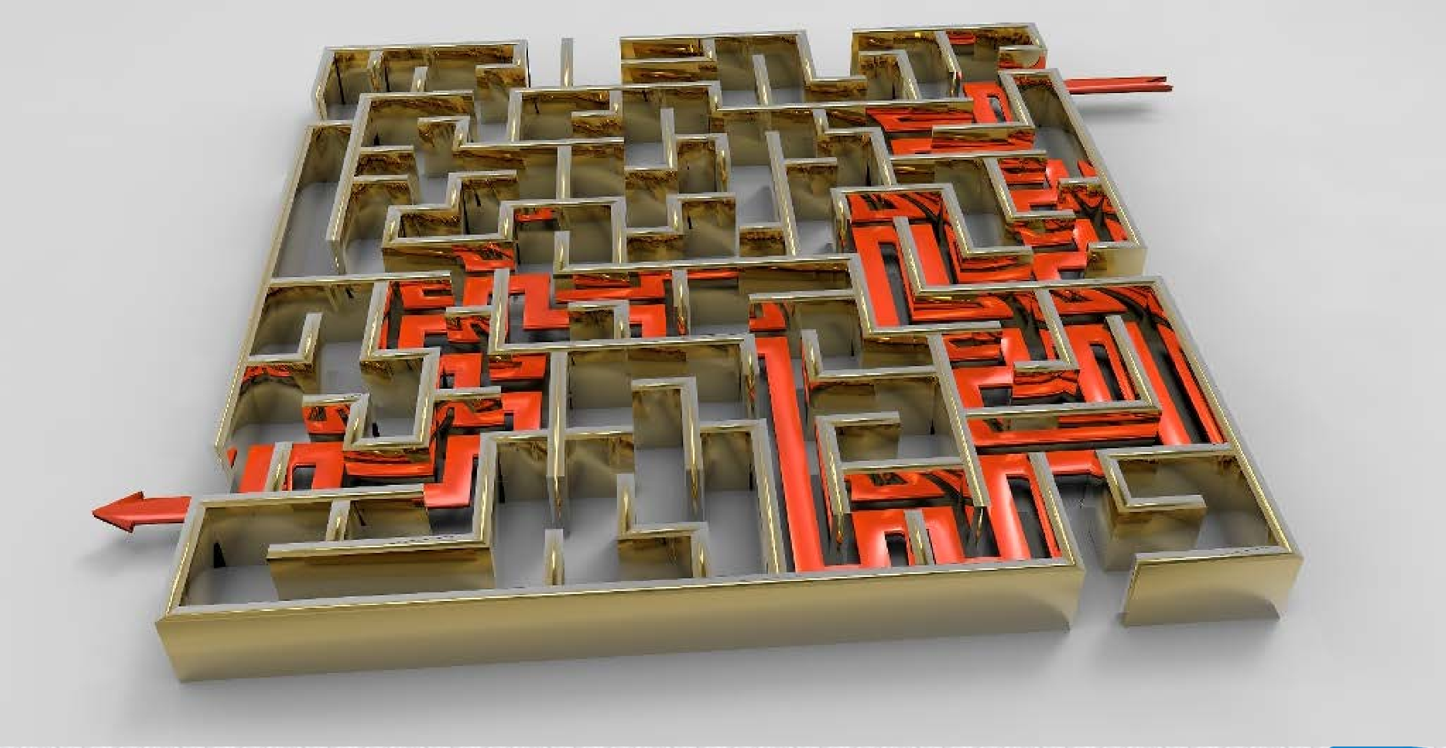
Disruption Begins With Planning

Influence Your Attackers' Actions and Decisions

Understand (And Fund) Your Priorities

Know What Belongs And What Doesn’t

Develop Capabilities, Not Tactics



Develop A Culture of Causality

Key Points

- Better planning enables effective response and disruptive ability
- Remember: time spent vs. return is a primary factor for attackers
- Knowing what's most important enables you to allow "acceptable loss" while thwarting the biggest threats to your business
- The ability to quickly detect outliers is key
- Develop repeatable skills and capabilities, not single-purpose weapons
- Practice to develop organizational "muscle memory" before you need it
- Don't stop until you've dealt with the root cause of the attack