ORO = Intel Gold
Making Strategic Threat Intel the Gold Standard in Business Risk Management

Sean Franklin & Brian Mohr
Project Far Side
It’s Maldonia Time
SITUATION

Project Far Side

▪ Sell our ACME Wadgets in Maldonia

▪ Timing is right
  – Market is ready
  – Under-served
  – Minimal competition

▪ Same business initiative
  – 2 versions of same company
  – 2 different outcomes
Your Presenters

Sean Franklin
- You treasure what you measure
- Desert Trail Dog
- More Fender than Gibson

Brian Mohr
- Pro Intelligence Requirement
- Soap-Boxer
- Recovering Jarhead
- Builds furniture in spare time
ACME 1: Diagnosis

Fortune 1000
- Global operations and markets
- Well governed & managed from BoD down
- Mature enterprise risk mgt program
- Full Info Sec program
  - Fairly mature
  - Dedicated threat intel team even!

However...
ACME 1 – Risk Mgt Structure

ERMC

Operational
Reg & Compliance
Fraud
Brand / Capital

$ Biz Unit $

Initiative 1
Far Side

InfoSec

ACME 1 – Risk Mgt Structure

RO

Risk Plan

RO

No ORO
No Bueno!
ACME 2: Diagnosis

- **Fortune 1000**
  - Global operations and markets
- Well governed & managed from BoD down
- Full Info Sec program
  - Fairly mature
  - Dedicated threat intel team even!
- Mature enterprise risk mgt program
  - *With 1 big change*

*This time... 😨*
ACME 2 – Risk Mgt Structure

$ Biz Unit $

Initiative 1

Far Side

Initiative 2

Operational

Reg & Compliance

Fraud

Brand / Capital

InfoSec

ERMC

Risk Plan

©2019 FireEye
What’s Changed?

Before

- $$$ Losses Experienced
- PRMM 😞
- Intel Lead?

After

- $$$ Loss Avoid
- PPMM 😊
- Intel Gold?
Lessons Learned
Challenges

Role ambiguity
- What’s IS ORO focused on?

Organizational resistance
- lack of understanding of strategic intel and value to the org

Turf battles
- addressing threats and risks dealing with fraud, physical operations & security concerns etc

Process & practice
- non existent / immature threat intel processes and lifecycle to support the role and function initially
Opportunities

Intel Gold
- move threat intel up the value chain from tactical to strategic focus
- orient CTI to actual biz problems; link to biz outcomes

Relationship oriented
- Mutual Success Model
- continual monitoring and reporting on early warnings based on PIR’s

Proactive
- Enhance IR plans and DR plans in accordance with RMP

Vendor Value
- Maximum value exploitation of intel sources and feeds
Start or Starting?

- Find a Sponsor
- Identify the right resource(s) to be your ORO
- Create or modify CTI practices & processes
- Scope your bounds
- Comm Planning
- Measure your effectiveness
Thank you 😊

sean@franklin-cyber.com

brian@d3intel.solutions