



CYBER DEFENSE SUMMIT 2019

ORO = Intel Gold

Making Strategic Threat Intel the Gold Standard in Business Risk Management

Sean Franklin & Brian Mohr



Sean Franklin
President - Franklin Cyber



Brian Mohr
Co-Founder D3 Intelligence



Project Far Side

It's Maldonia Time

SITUATION

Project Far Side

- Sell our ACME Widgets in Maldonia
 - *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

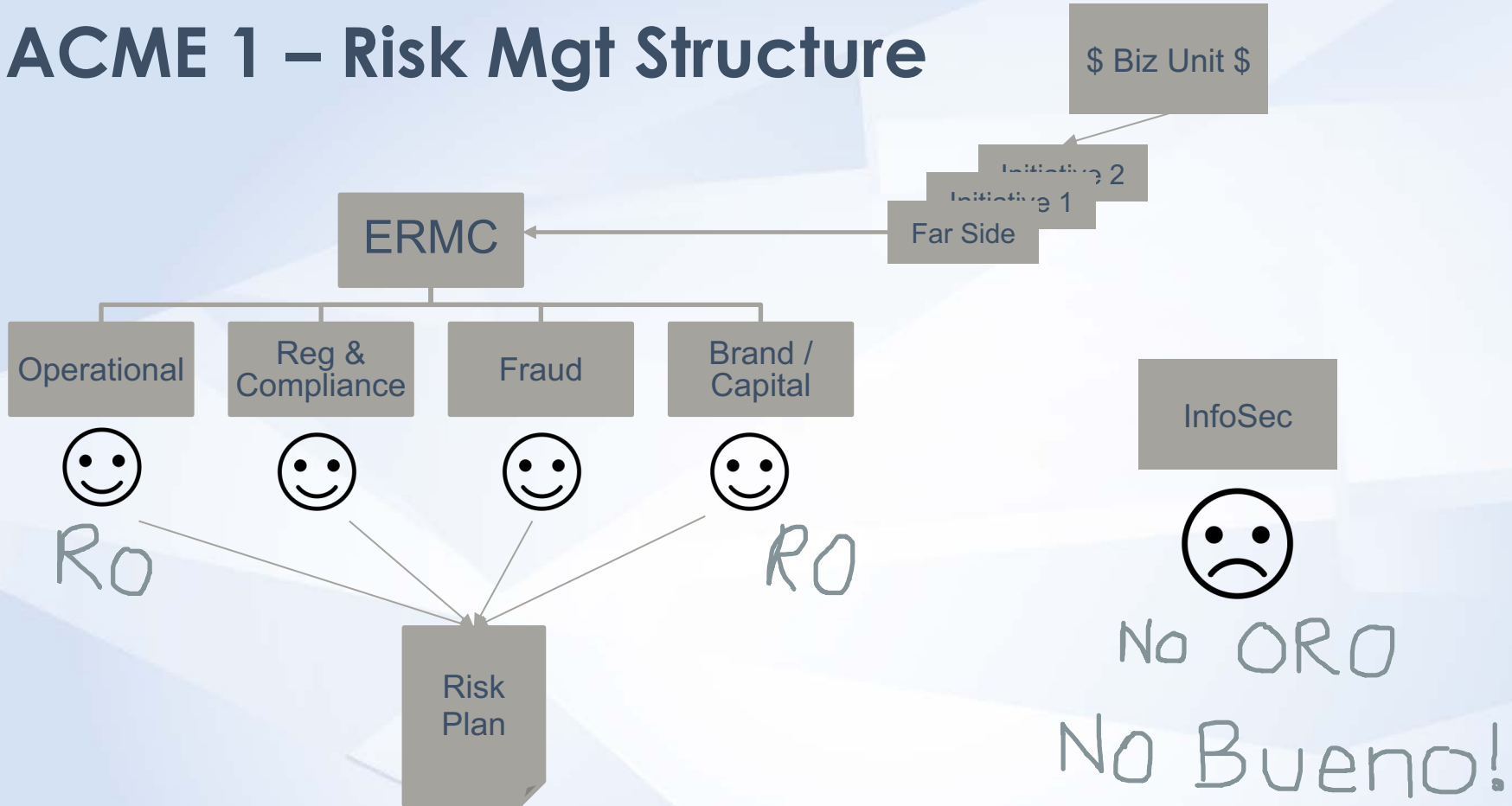
- *Global operations and markets*
- Well governed & managed from BoD down
- Mature enterprise risk mgt program
- Full Info Sec program
 - *Fairly mature*
 - *Dedicated threat intel team even!*

However...



Where The World Wadgets!

ACME 1 – Risk Mgt Structure





ACME 2: Diagnosis

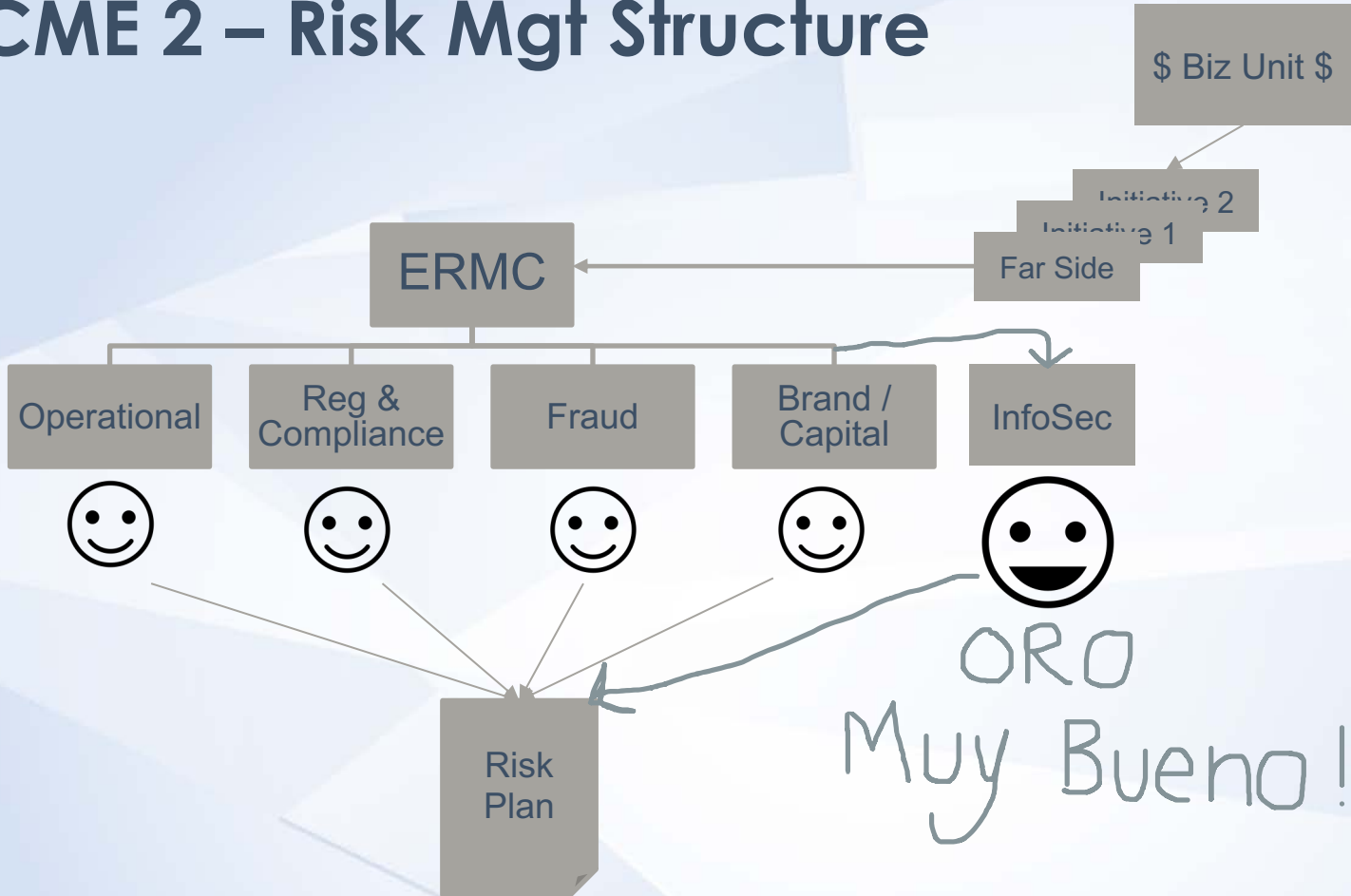
- **Fortune 1000**
 - *Global operations and markets*
- Well governed & managed from BoD down
- Full Info Sec program
 - *Fairly mature*
 - *Dedicated threat intel team even!*
- Mature enterprise risk mgt program
 - ***With 1 big change***

This time... 



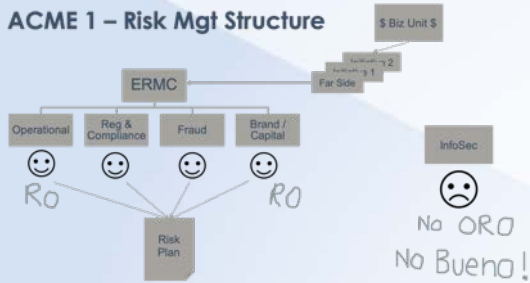
Where The World Wadgets!

ACME 2 – Risk Mgt Structure



What's Changed?

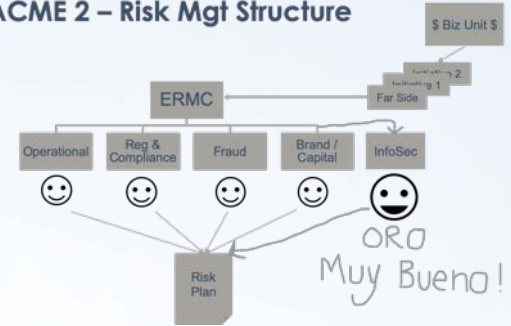
ACME 1 – Risk Mgt Structure



Before

- \$\$\$ Losses Experienced
- PRMM ☹️
- Intel Lead?

ACME 2 – Risk Mgt Structure



After

- \$\$\$ Loss Avoid
- PPMM 😊
- Intel Gold?

Where The World Wadgets!

Lessons Learned

The background features a complex, abstract geometric design. It consists of various overlapping shapes in shades of blue and grey. On the right side, there are several prominent shapes, including a large, light blue circle, a grey rectangular block, and a series of parallel lines forming a grid-like pattern. The overall aesthetic is modern and technical.

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

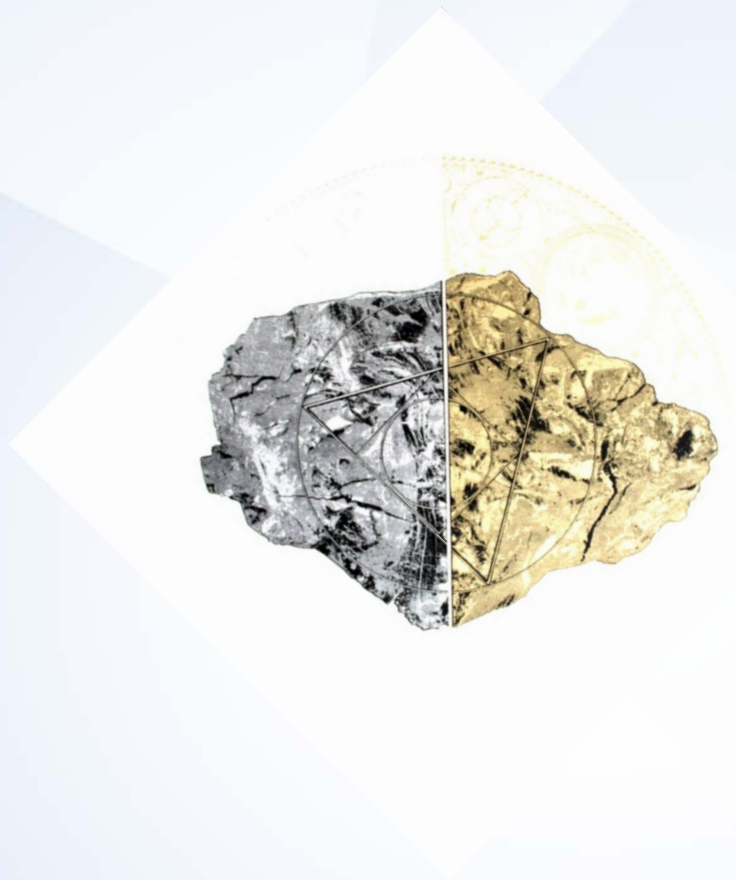
- Enhance IR plans and DR plans in accordance with RMP

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





CYBER DEFENSE SUMMIT 2019

Thank you 😊

sean@franklin-cyber.com

brian@d3intel.solutions