IRM

Cyber Risk Management: Bringing Order to Chaos

Peter Gouldmann

U.S. Department of State
Bureau of Information Resource Management

Oct 2017

Chaos Reigns

- Equifax
- U. S. Office of Personnel Management
- HBO/Sony Pictures
- Target
- Global Petya Ransomware
- … and others.

All thought everything was fine – but was it? Probably not…

IRM

The Myth

- We're safe, the Internet has BILLIONS OF USERS (anonymity).
- Cybersecurity is very important to us – we hired a CISO.
- If it isn't a matter of IF but rather WHEN, we'll take our chances.
- We spent a fortune on the BEST NETWORK SECURITY PRODUCTS; we're safe.

We have to close every hole, they only have to find one!

IRM

The Reality

Systems and software will be weak for the foreseeable future

- Patching is problematic
- Legacy IT limits ability to protect

Threat actors increasing in numbers and capabilities

- Persistence is real – if you patch late they may already be inside.
- Actions progressing from can I get in, to what can I take, to now what can I damage.
- State-Sponsored, Hacktivists, Criminals, benign and malicious insiders, etc.

Advantage Threat Actor!

IRM

Past Efforts

A summary of a CISO conversation with the CEO and Board Chair…

You request a budget to protect the network. You receive all the funds you requested and build out your security protections. You have anti-malware and endpoint capabilities. You feel pretty confident. The CEO and Board Chair asks if everything is good now. You say you feel confident but there is no guarantee. They ask what more can be done. You say you can add more capabilities from the experimental area. The conversation repeats in 6 months. Now what?

You just accept the risk right?

IRM

How do we conduct business then?

Focus on Risk Management

- Stop using IT? No, well….err… yes a little!
- There are lessons in how to address adversarial attacks.
  - Recognize and accept the reality of the situation
  - Focus attention on what is likely to cause the greatest harm first
  - Work to improve the situation whenever and wherever possible and practical. (risk vs. reward/loss)

How much can you afford to lose?

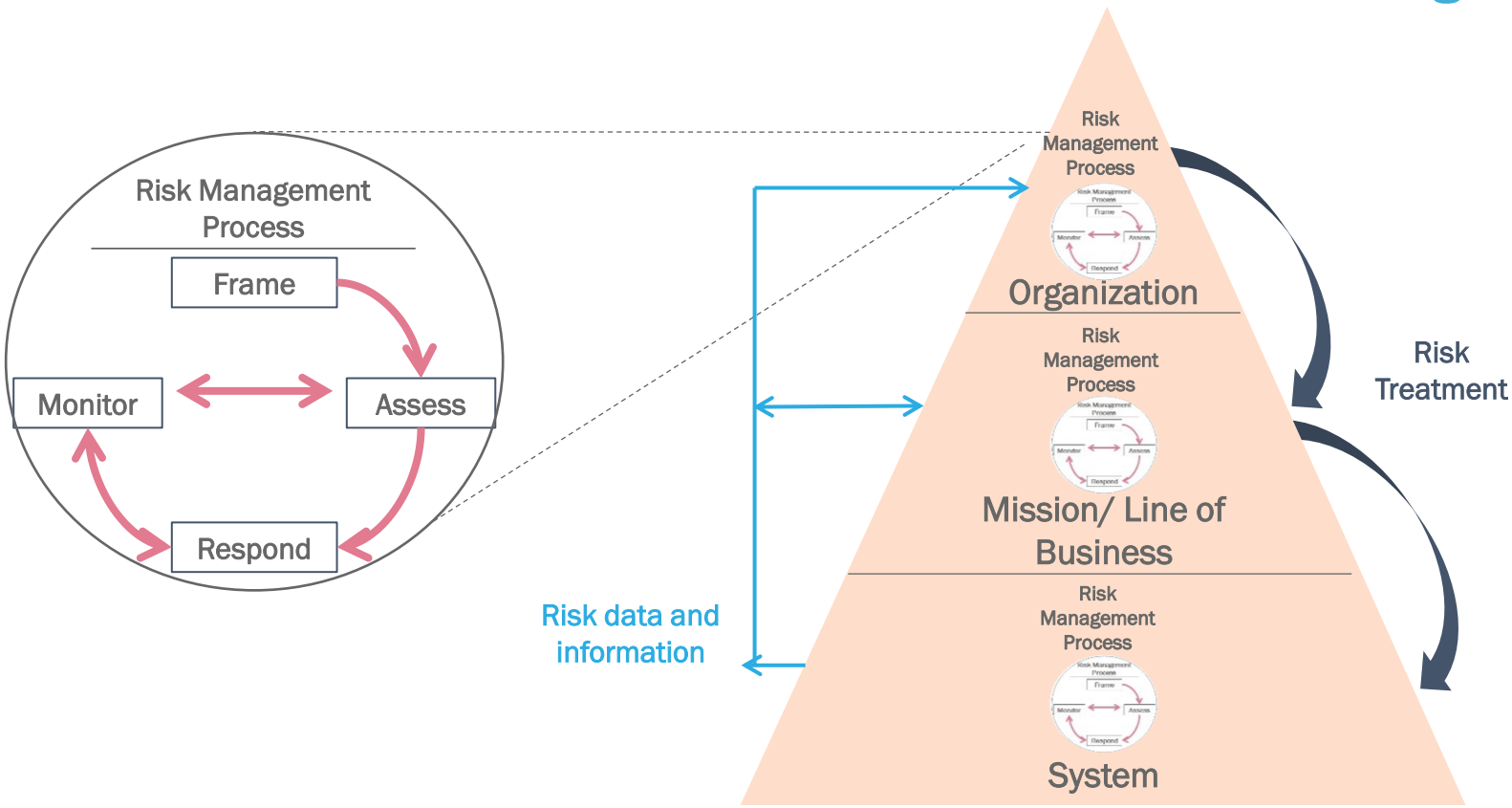
- Money, Reputation, Harm to Others?

Risk is inherent in all aspects of business and mission operations!

IRM

How does it work?

Fulfilling Risk Management Strategic Goals:
Define What Matters – Govern – Measure – Decide- Manage



This model enables the Department to frame, assess, respond to, and monitor risks independently at each level—Organizational, Mission, and System.

Risk Treatments

Start simple and move to complex actions –

- Look at business process resiliency.
- Update software and patch often
- Train users in phishing and significantly limit privileges.
- Re-architect flat networks into segments of business activity

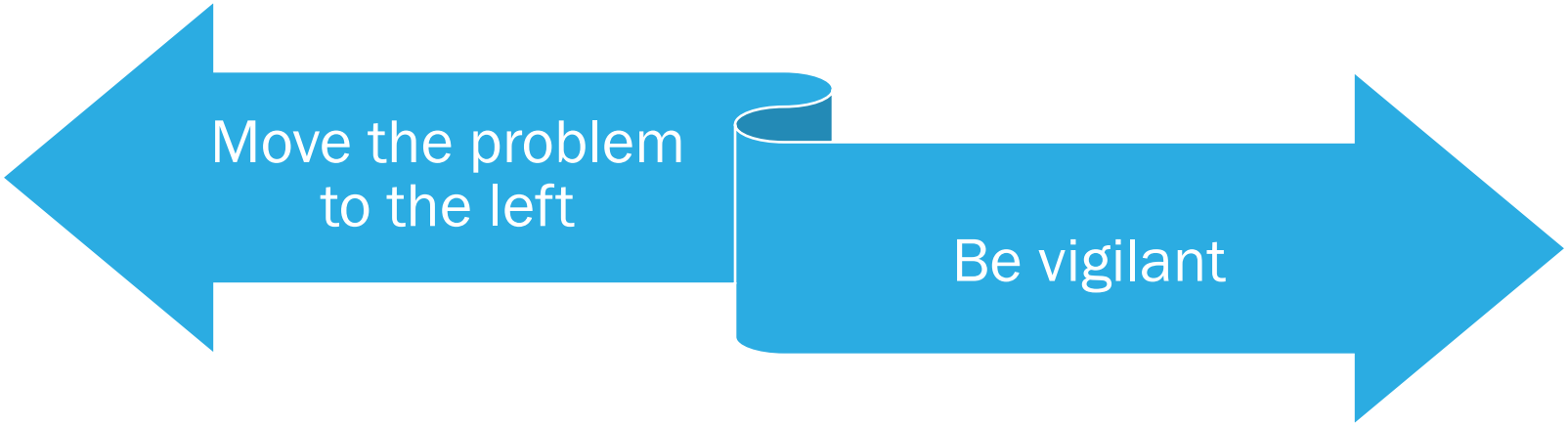
Other things to help –

- Rate organizations on level of diligence
- Draft standard contract language
- Develop scoring model for investments
- Move the risk conversation to the business and mission managers

IRM

Unacceptable Result

What if you do this and you aren't happy with the results – what then?



Consider another approach:

- Know what risk is ok and use that in your planning
- Build and buy smarter

If you must operate with unacceptable risk:

- Monitor for problems frequently
- Train and be ready to respond
- Have a fallback plan
- Know how to recover to normal business
- Make plans to change the situation to lower the risk

IRM

Key Takeaways

Know your mission or business

- What drives revenue is key to accomplish your goals

Characterize your specific threats

- SWOT – minus S and O

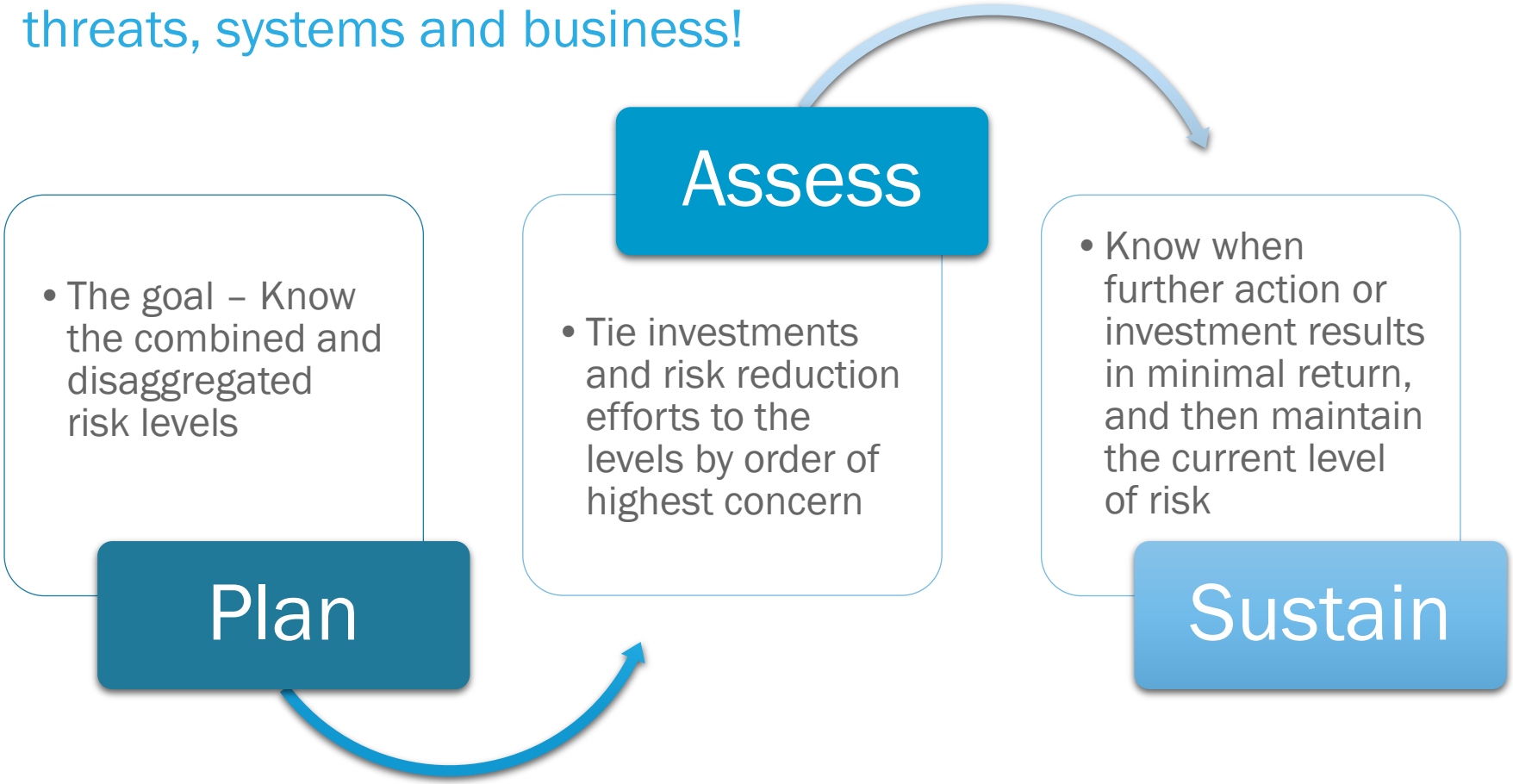
Plan risk treatments appropriate for the level of unacceptability

- Insurance
- Line of business resiliency
- System remediation

IRM

Key Takeaways (continued)

Be vigilant of change – threats, systems and business!



Questions?