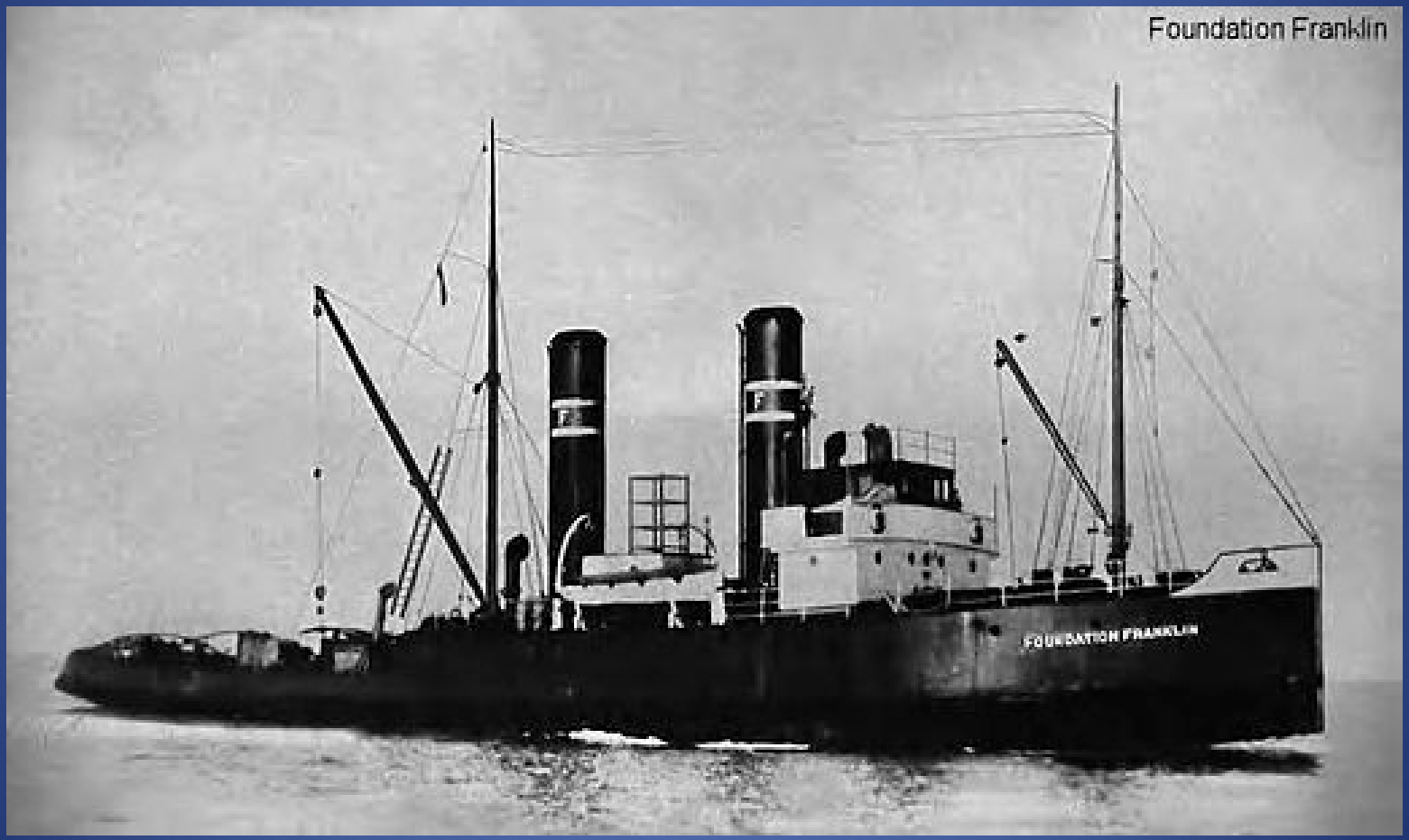
Managing Cyber Risk

Captain Andrew E. Tucci

U.S. Coast Guard

Ships Then



Ships Now

Sources of risk

- Exploding boilers and mechanical failures
- Heavy weather and navigation hazards
- Human factors
- Cyber hazards – an unknown, but certainly growing portion of our total risk
- Cyber is a SAFETY issue, not just security

What Makes Cyber Risk Special?

Vulnerability increases with every new device

Threat is unlimited

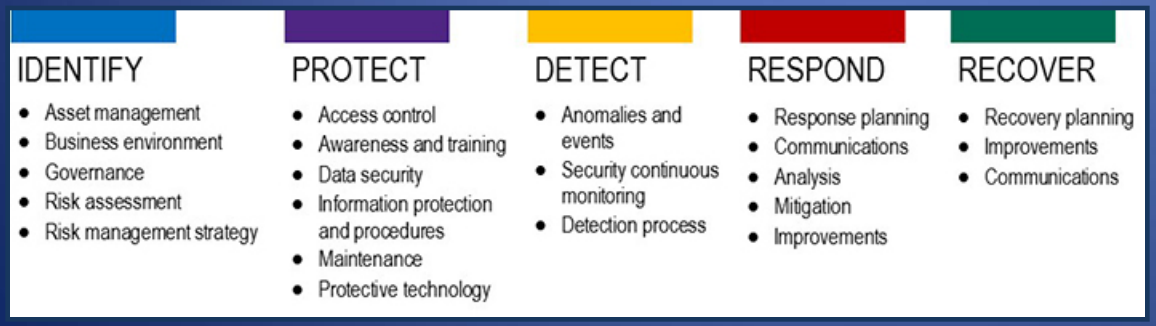
Likelihood of an incident is near certain

Detection is a factor

rapidly growing portion of our total risk exposure

Coast Guard Approach

- Cyber as a leadership responsibility
- Team approach to risk identification/mitigation
- Authority limited to MTS issues, interest limited to those with potentially significant consequences
- NIST Framework (holistic approach)
- Include procedures in MTSA plans, ISM system, etc
- Promote and develop a cyber safety culture



Flexible approach on vulnerability and consequences

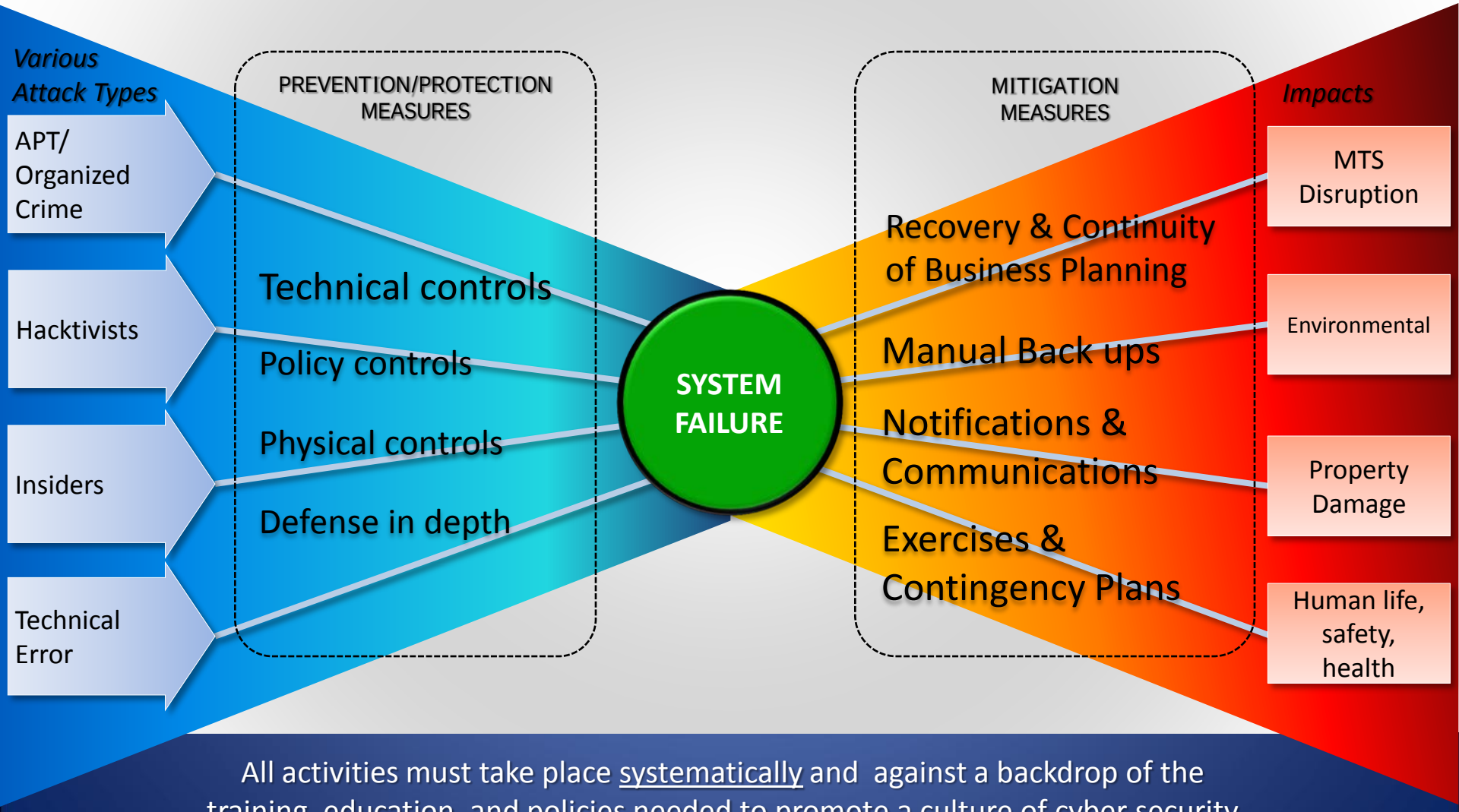
- Engineering Solutions
- Training and company policies
- Physical Access control
- Technical solutions
- Manual back ups
- Recovery and resilience planning
- Exercises

Next Steps and Challenges

- Coast Guard Cyber Strategy June 2015
- Draft voluntary policy (NVIC) August 2015
- Final policy January 2016

- Quantifying the risk
- Keeping up with rapidly changing systems
- How to do effective oversight
- Resources and training for CG personnel

Cyber Security Risk Model



All activities must take place systematically and against a backdrop of the training, education, and policies needed to promote a culture of cyber security

Questions?