FAIR CONFERENCE 2019

# Closing the Risk Management Loop with Cyber Risk Quantification


**GREG ROTHAUSER**

Enterprise Business Information Security Officer (BISO),
MassMutual

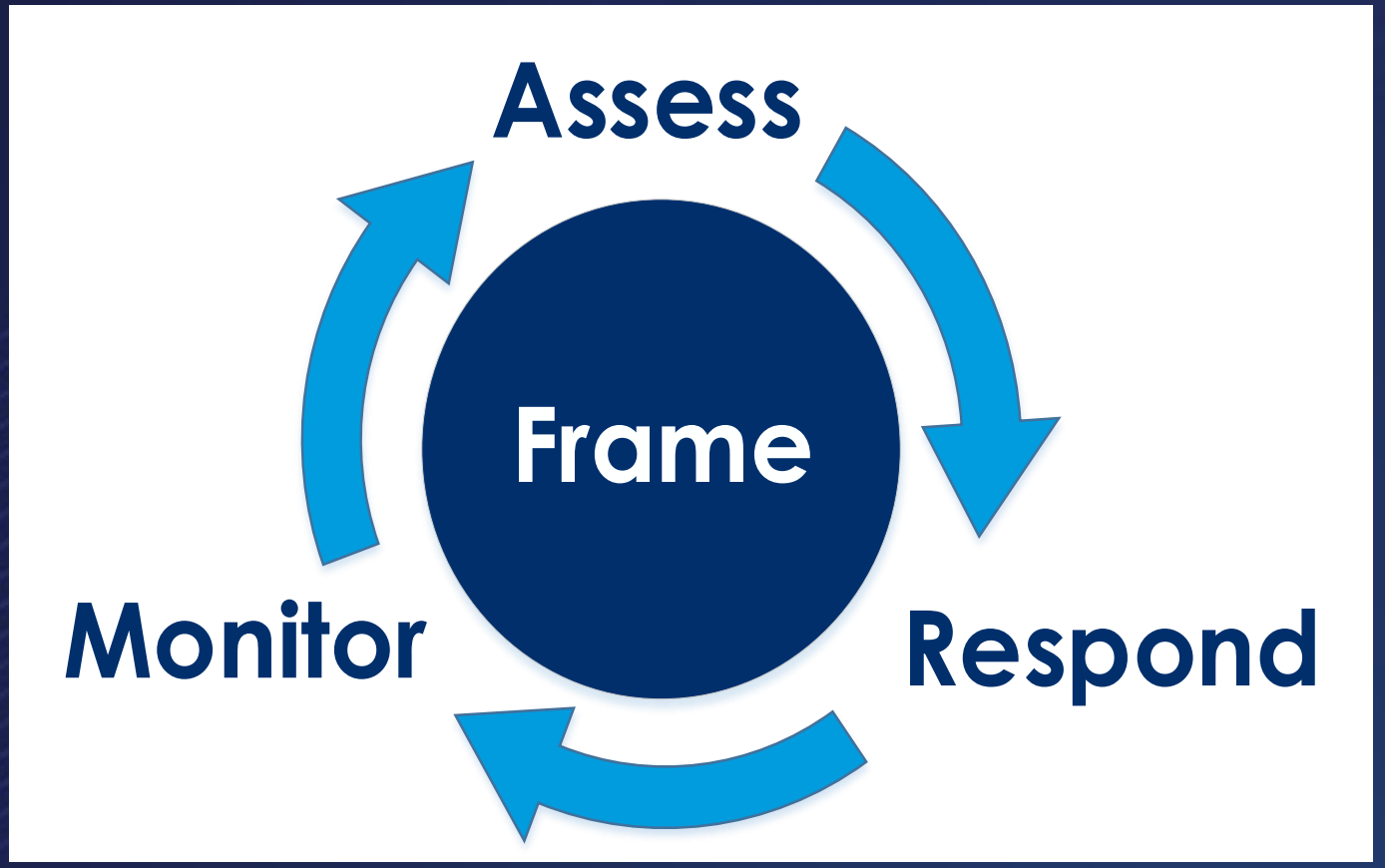
# Closing the Risk Management Loop with Cyber Risk Quantification

FAIR CONFERENCE 2019

# Closing the Risk Management Loop with Cyber Risk Quantification

FAIR CONFERENCE 2019


# Risk Management Process - NIST



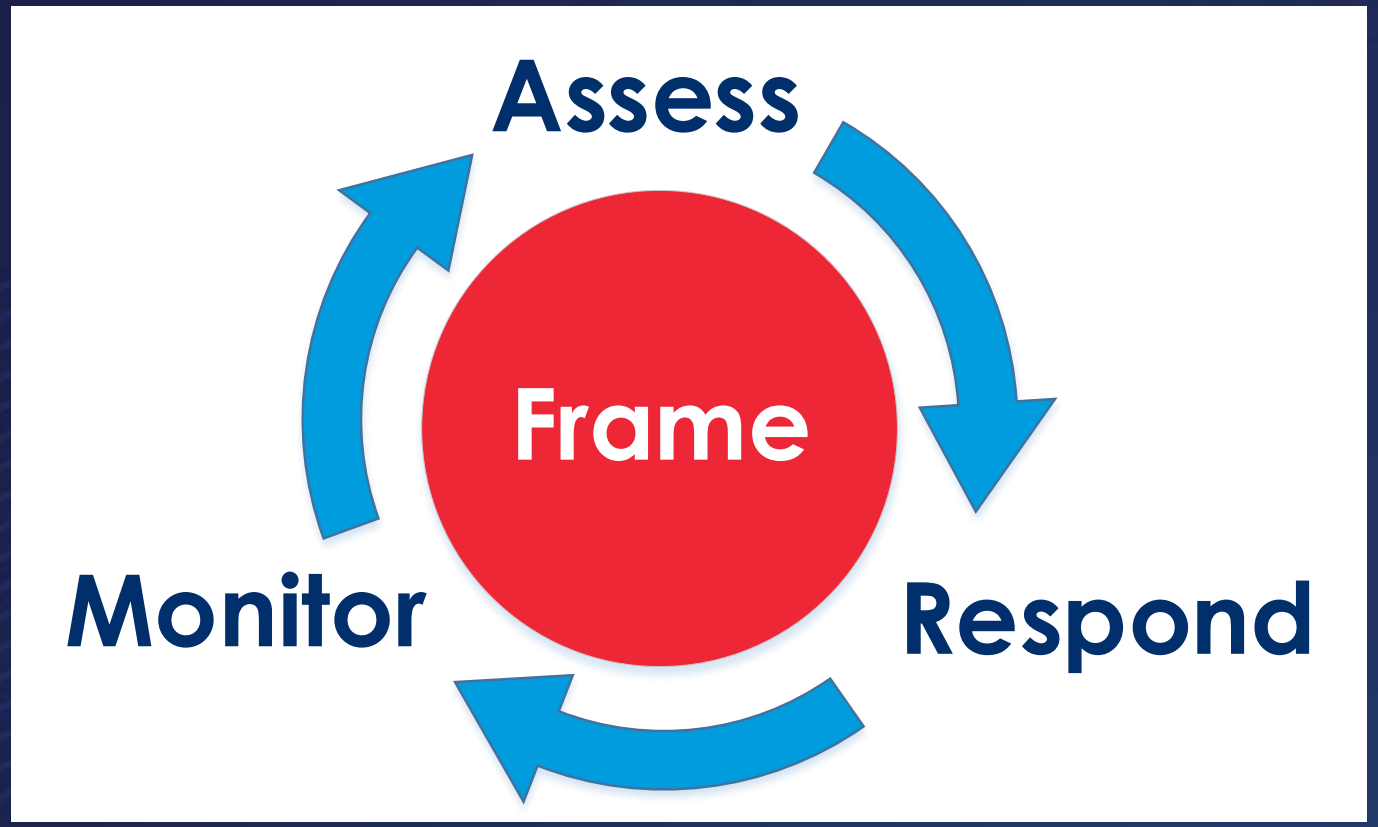

Modified from NIST SP800-30 Guide for Conducting Risk Assessments

# The Methodology – Factor Analysis of Information Risk (FAIR)

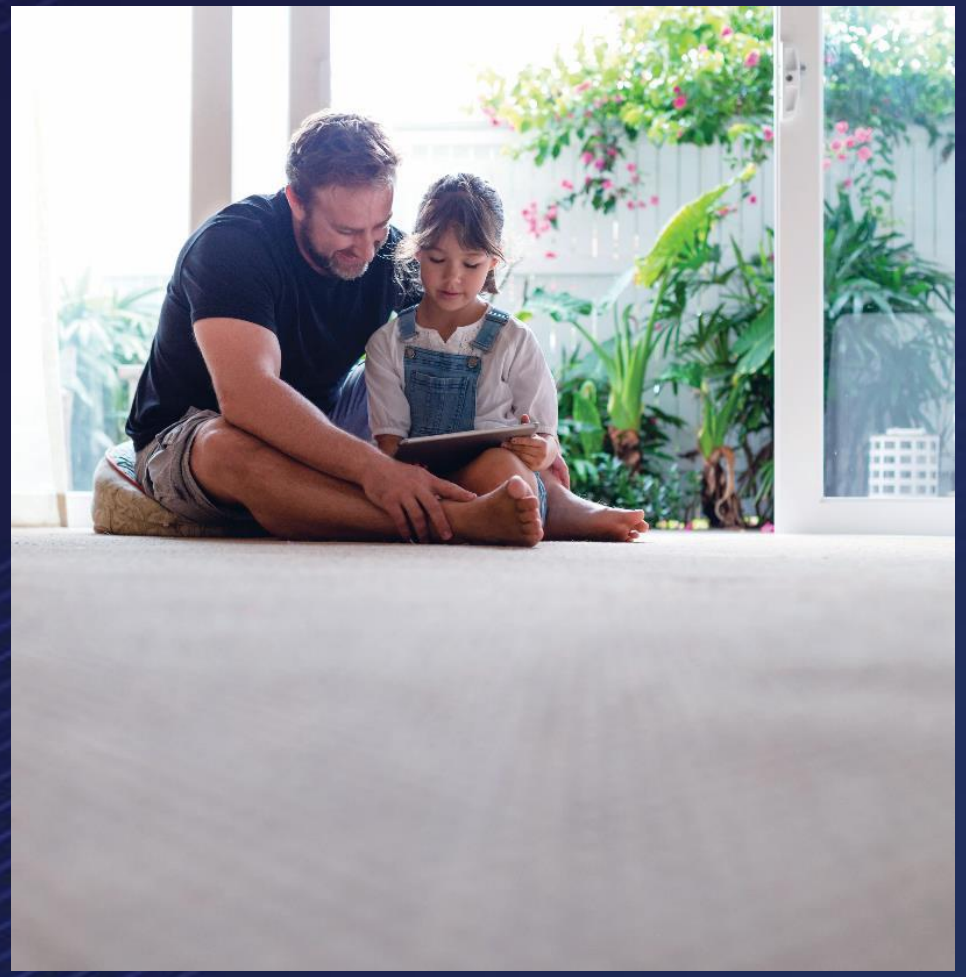
FAIR CONFERENCE 2019


Facilitates better analysis by breaking risk down into discreet components

FAIR INSTITUTE



# Risk Management Process - Frame

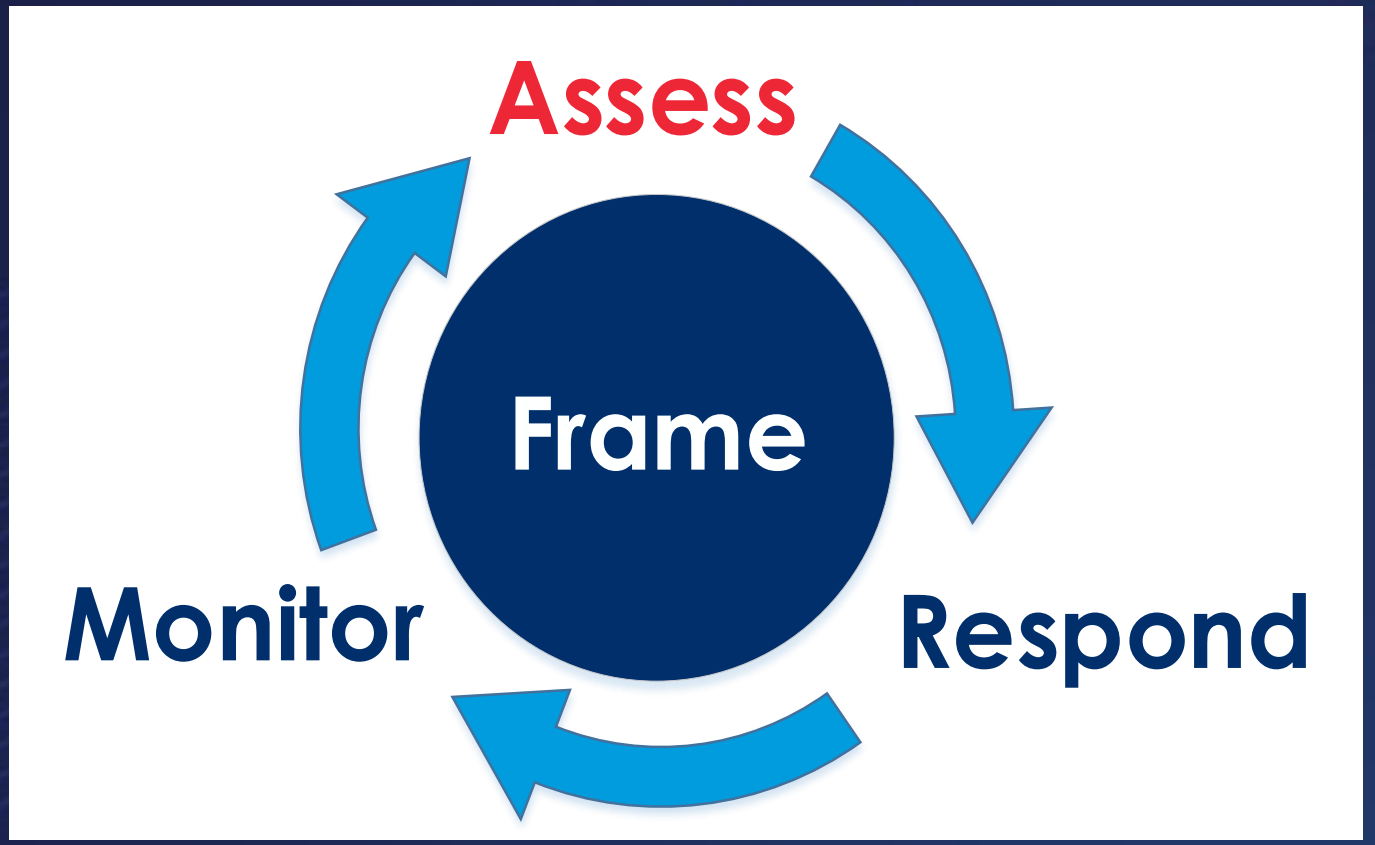


- Policies & Standards
- Processes
- Assets
- Methodology (FAIR)
- Risk Appetite

# Risk Appetite

FAIR CONFERENCE 2019

- Often this comes from the business and are broad statements: "We don't want to impact more than 1,000 customers." "We don't want to wind up on the news."
- Can look at actual incident response and lessons learned remediation
- Can have multiple thresholds
- Individual lines of business or organizational divisions can have their own



# Risk Management Process - Assess

FAIR CONFERENCE 2019

## Traditional Qualitative Approach

| | |
|---|---|
| HIGH | Cloud |
| HIGH | Tech Debt/Legacy Systems |
| HIGH | Vulnerability Management |
| HIGH | Ransomware |
| MED | DDoS |
| MED | Insiders |

From a FAIR perspective, none of these are risks.

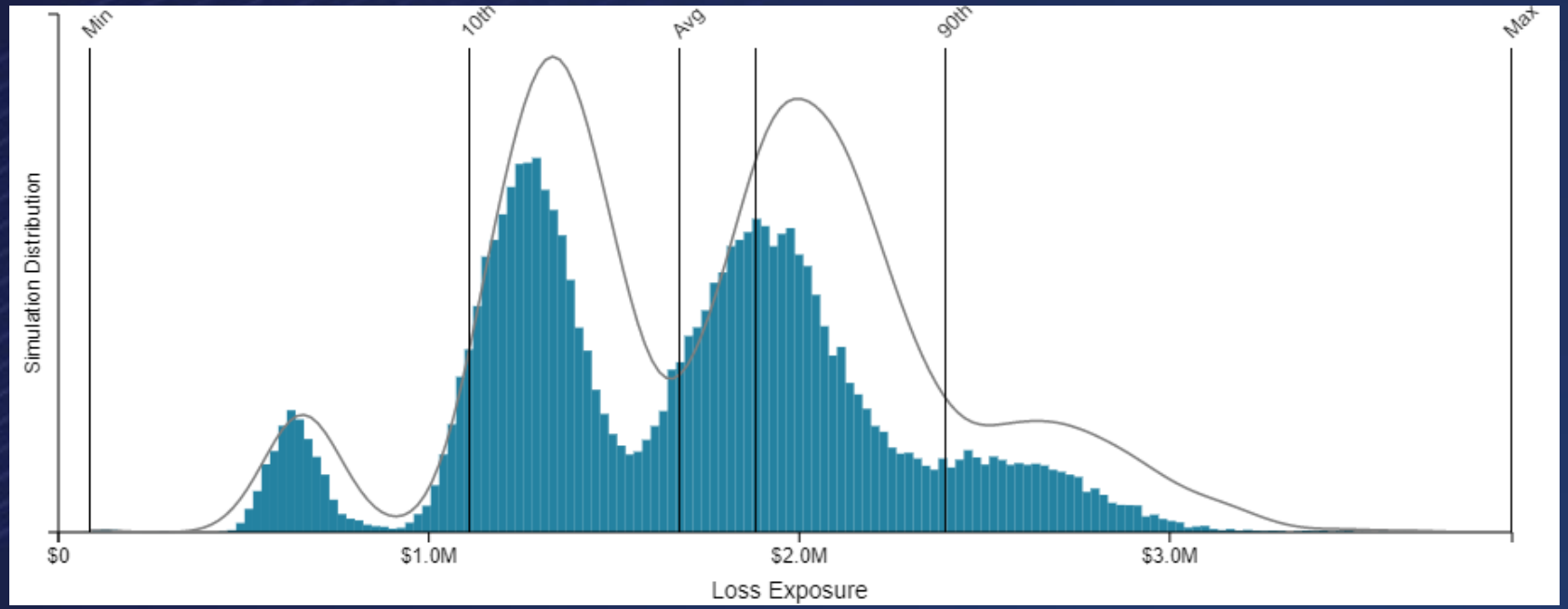
Risks are defined as events that incur financial loss for the organization.

# FAIR Methodology View of Risks

FAIR CONFERENCE 2019

Ransomware designed by cybercriminals encrypts business critical systems

| 10th Percentile | Most Likely | 90th Percentile |
|---|---|---|
| $1.1M | **$1.9M** | $2.4M |
| Min $87K | Average $1.7M | Max $3.9M |







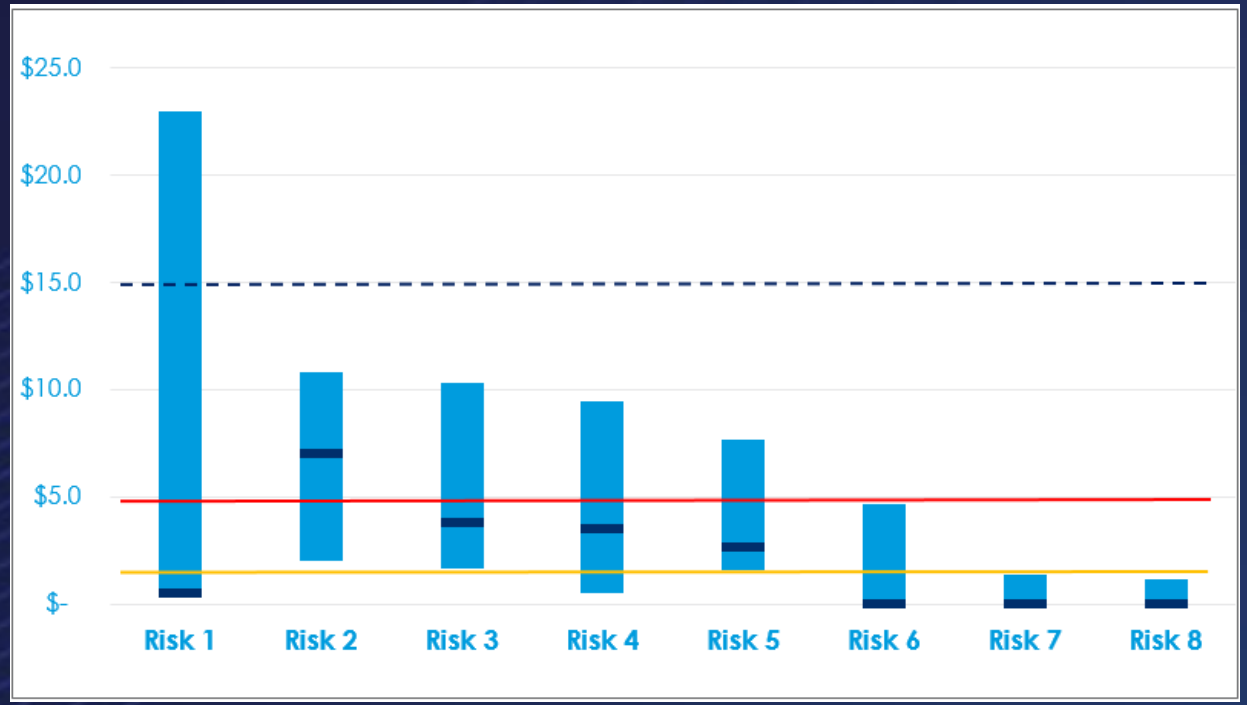
#FAIRCON19

# Risk Management – A Quantitative View

FAIR CONFERENCE 2019

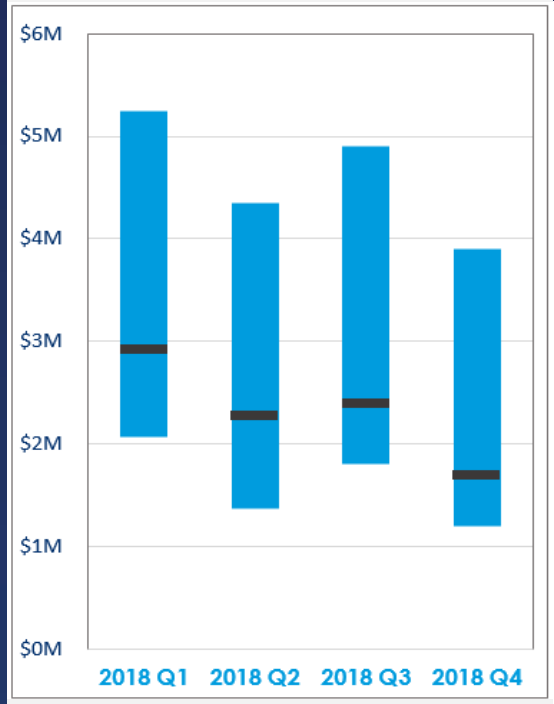
## Risk Appetite

scenarios above early warning levels




## Risk Exposure Trend

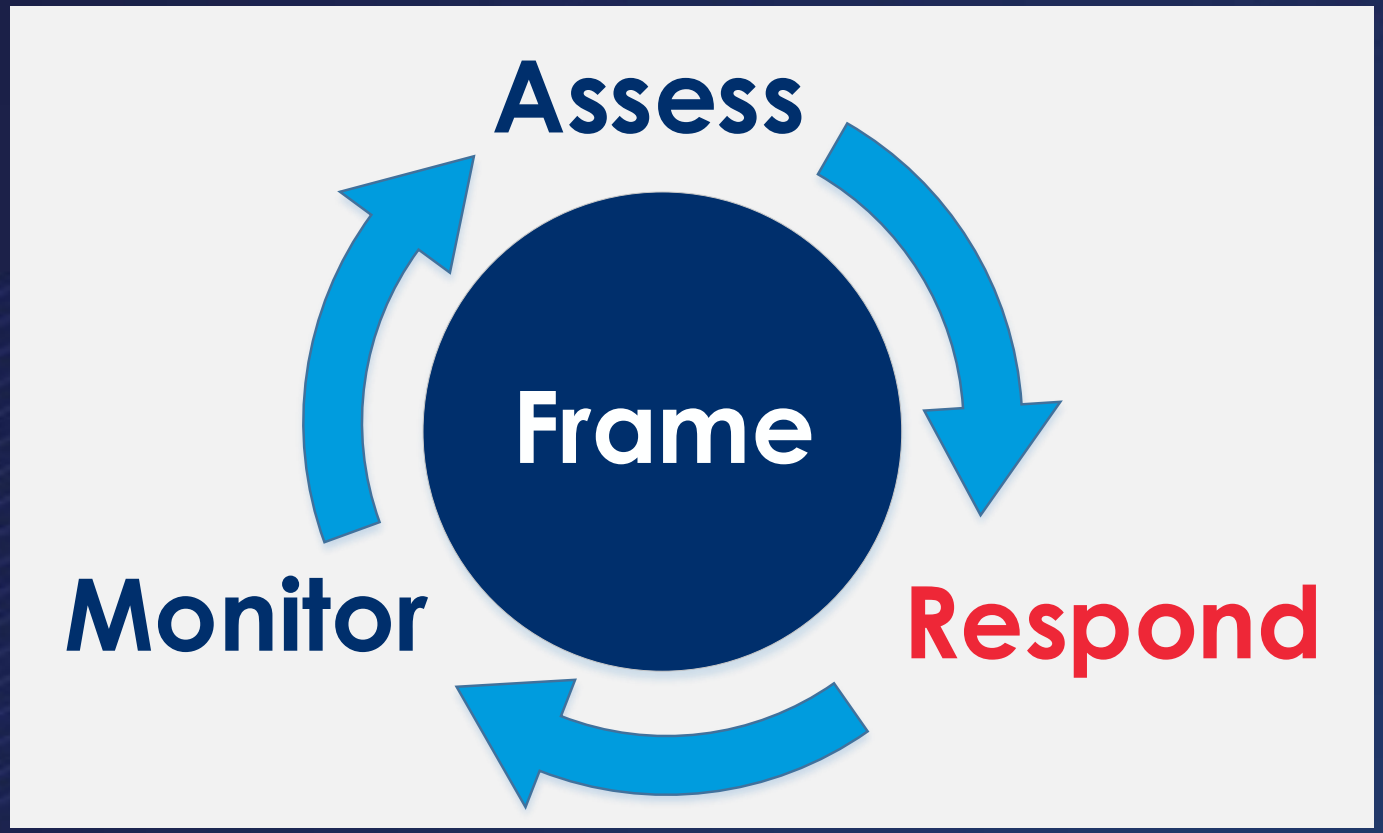
aggregated scenarios*



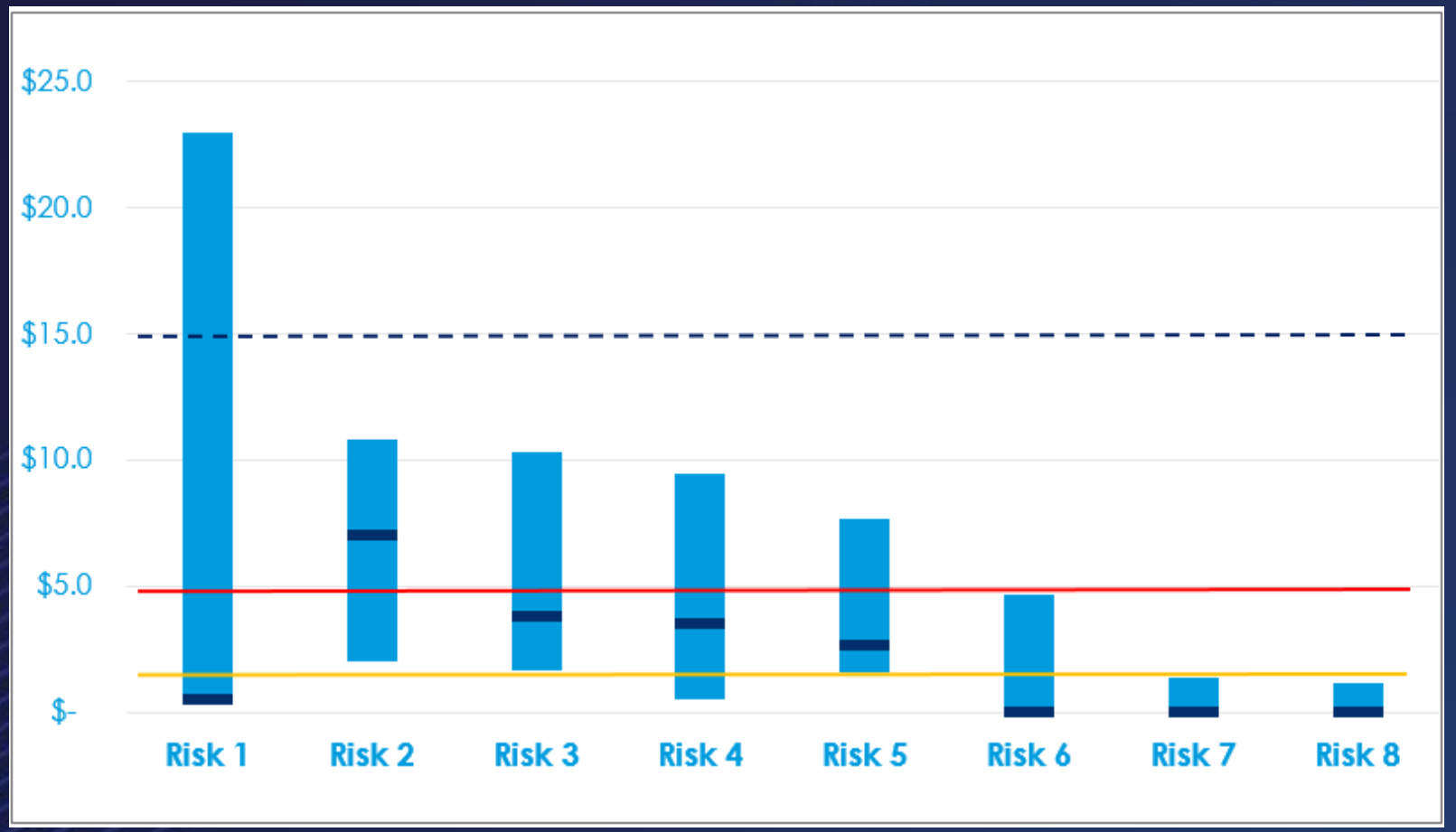

* Includes only scenarios above Early Warning level




#FAIRCON19



# Risk Response – Prioritization




Is the Risk fairly low but with the capacity to explode?

Can it be accepted?

Do you have a clear "leader" that needs to be addressed first?

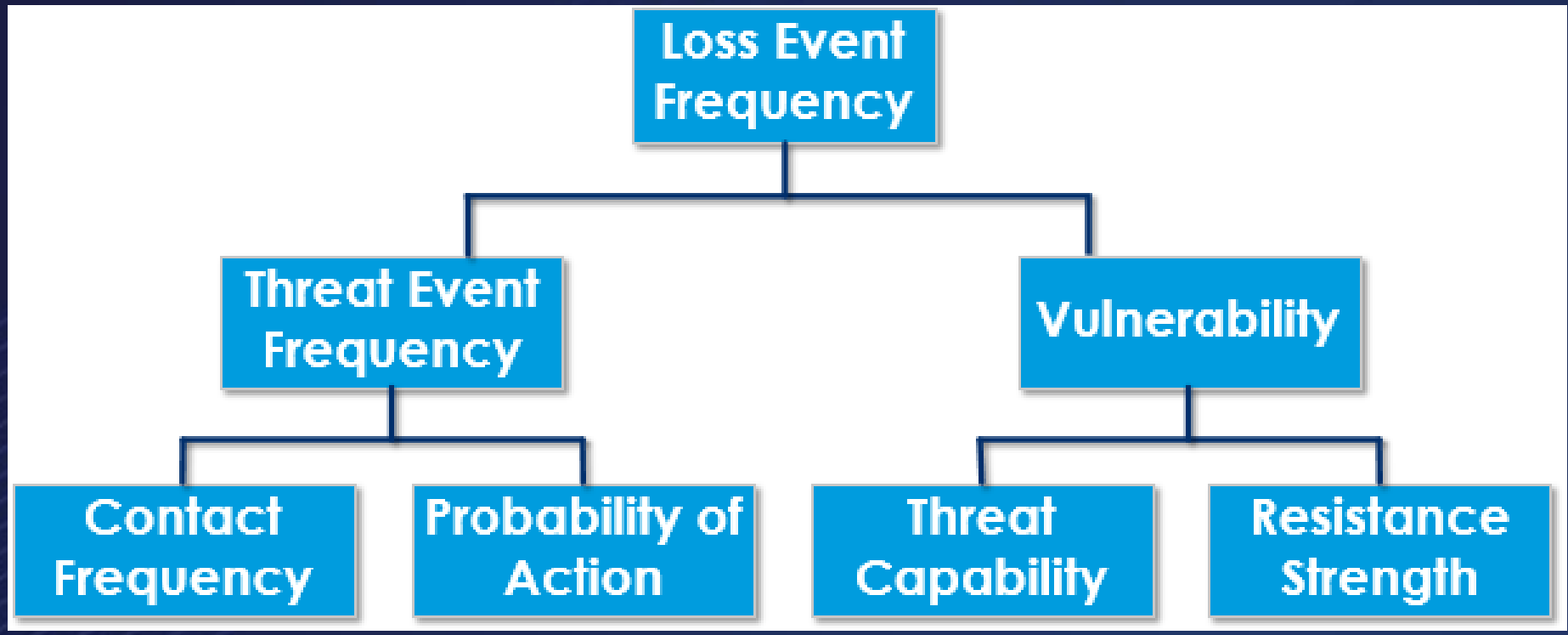
# Risk Response – Mitigation Strategy

FAIR CONFERENCE 2019

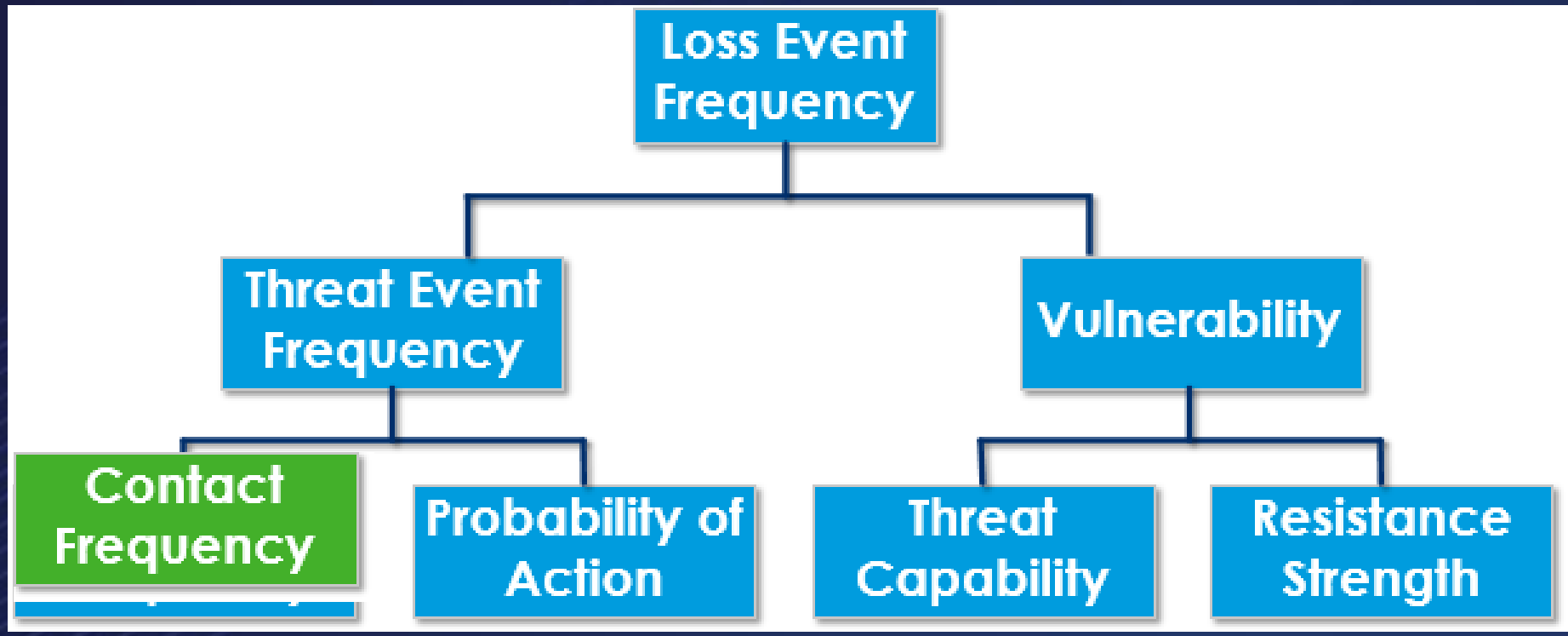
Ransomware designed by cybercriminals encrypts business critical systems

To mitigate risk, the Loss Event Frequency, the Loss Magnitude, or both need to be reduced

# Risk Response – Mitigation Strategy

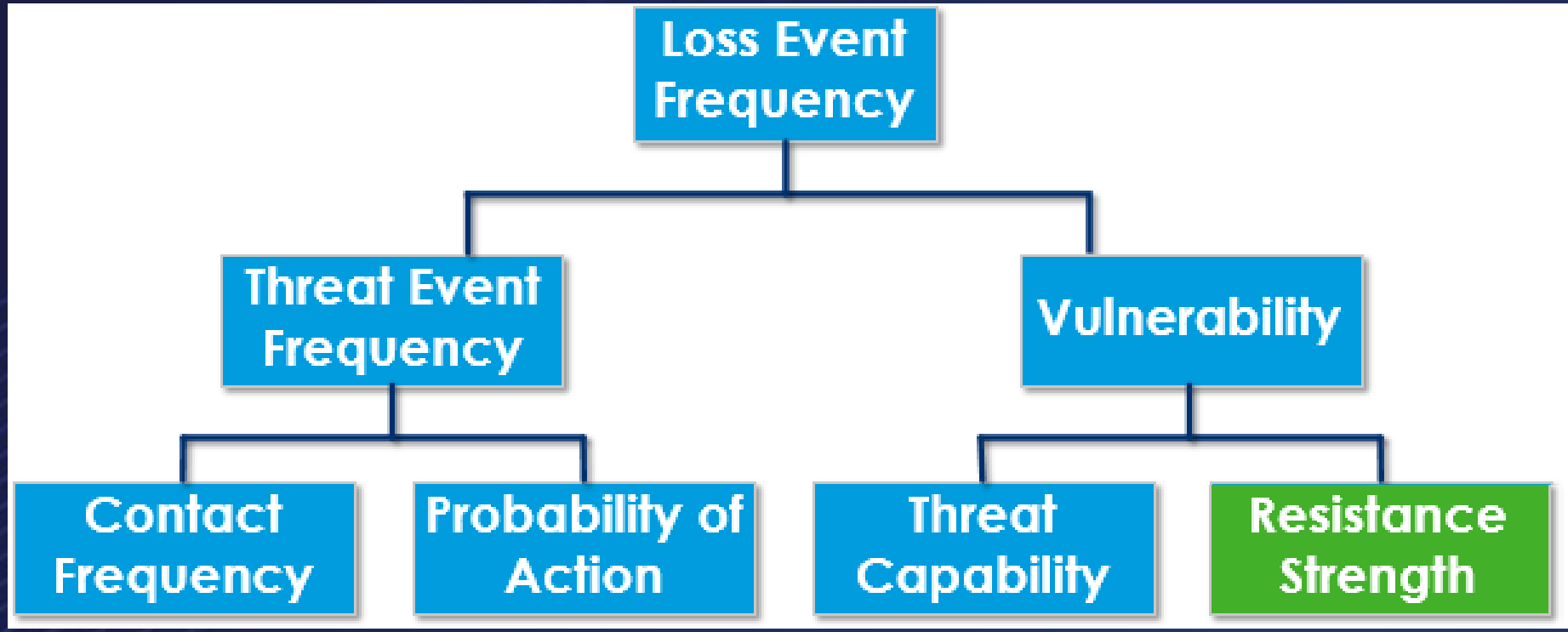


# Risk Response – Mitigation Strategy



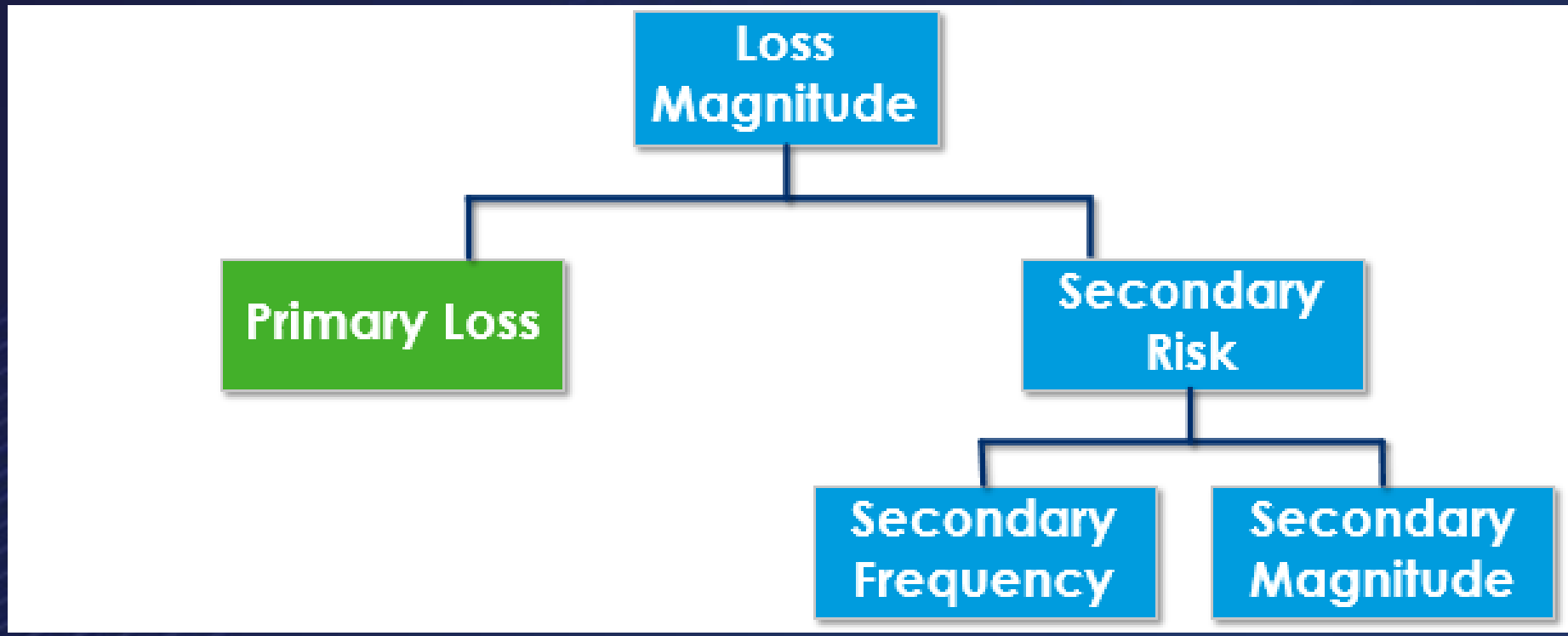

Establish network segmentation, restricting contact to business critical systems or data

# Risk Response – Mitigation Strategy



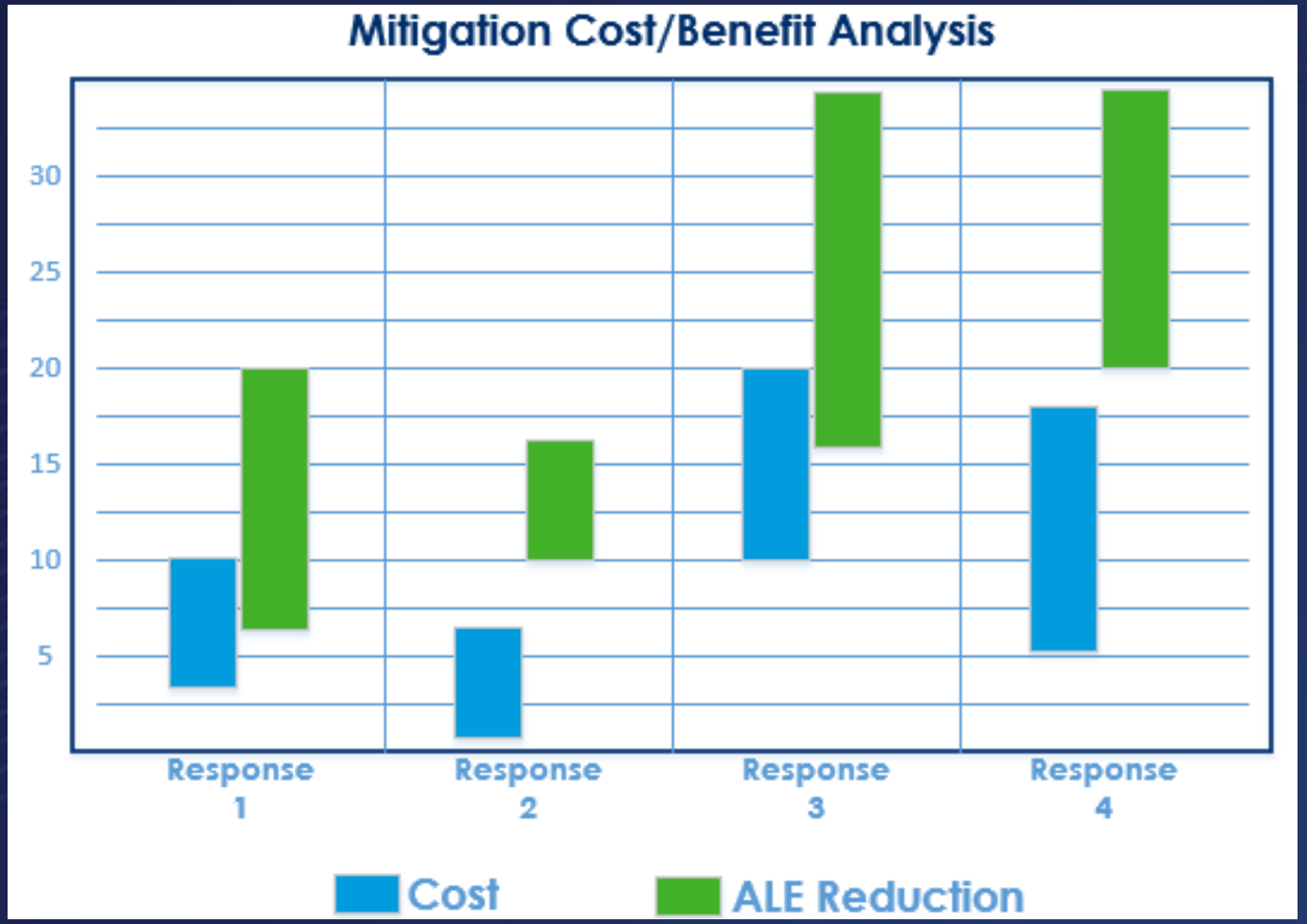

Improve system patching and tighten access controls

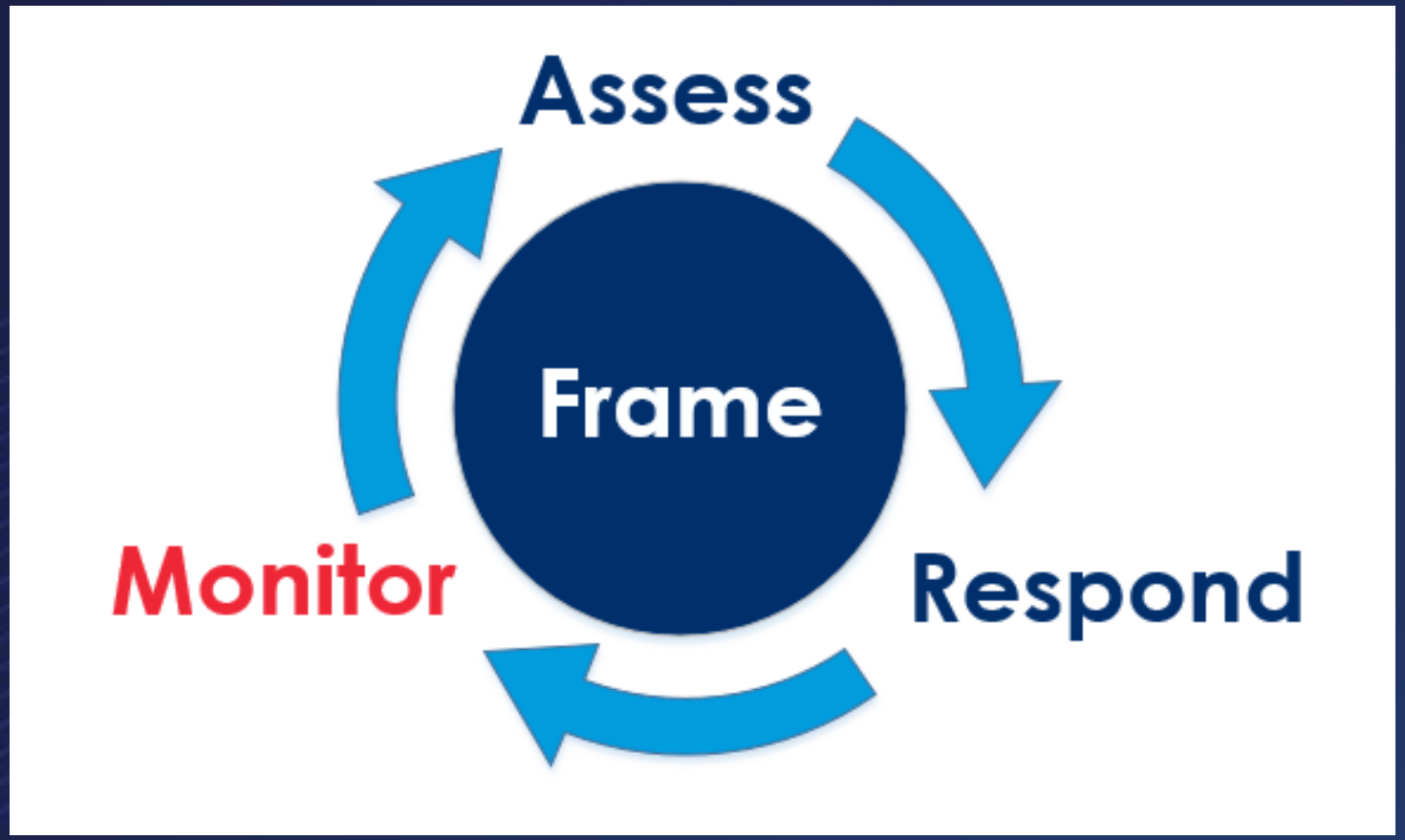
# Risk Response – Mitigation Strategy




Behavioral Analysis to Identify and Respond to Encryption Before Completion

# Risk Response – Infomred Decision



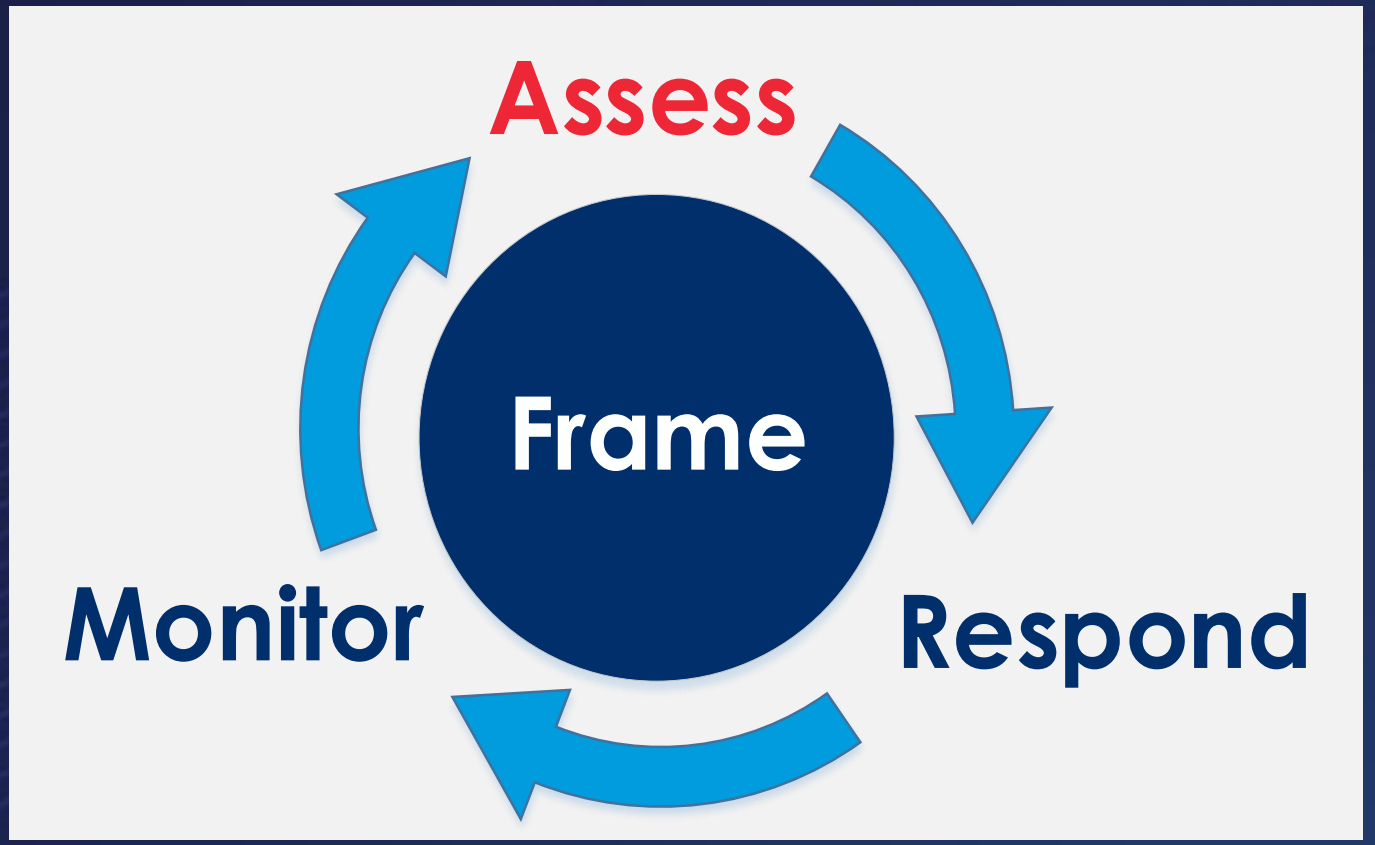


# Risk Response – Monitor

| Metric | Effect |
|---|---|
| % of critical file servers segmented | Contact Frequency |
| # of users with write access to critical file shares | Resistance Strength |
| # of unpatched high & critical vulnerabilities | Resistance Strength |
| Average time to respond for rapid file encryption | Loss Magnitude |
| Tested RTO and RPO for critical system | Loss Magnitude |

As Metrics Change, We Can Measure the Resulting Change in Risk Exposure

Showing Progress… or Highlighting New Areas of Risk/Focus


Assess
Frame
Monitor
Respond

FAIR CONFERENCE 2019

# Questions?