FAIR CONFERENCE 2019

Defining the Goals of an Effective Risk Management Program

Moderator: JACK JONES
Chairman,
FAIR Institute

EMERY CSULAK
Deputy CIO & CISO,
U.S. Department of Energy

CHRISTOPHER PORTER
CISO,
Fannie Mae

JOEY JOHNSON
CISO,
Premise Health

OMAR KHAWAJA
CISO,
Highmark Health

Copyright 2019 FAIR Institute, Inc.

Omar's Tips for Effective Risk Management

FAIR CONFERENCE 2019

- **Measurable**: compare different business units to each other and track historical trends
- **Audience-centric**: must be in language the business can grasp; must convey meaning that leads to some sort of conclusion or objective judgement
- **Aligned**: must map to other parts of the Cyber program, e.g.: controls, audits, compliance, vulnerabilities, etc.
- **Rational**: there must be robust defensible underlying logic to explain the results that are reported
- **Decision support**: results should simplify selection of appropriate options in decision making / prioritization process

Copyright 2019 FAIR Institute, Inc.

Chris's Tips for Effective Risk Management

FAIR CONFERENCE 2019

- Understand that **cyber risk is business risk**
- Get the organization to **speak the same risk language**
- **Identify top risk scenarios** facing the organization and quantify loss exposure
- **Prioritize investments** to mitigate scenarios with greater loss exposures

Copyright 2019 FAIR Institute, Inc.

Emery's Tips for Effective Risk Management

FAIR CONFERENCE 2019

- **Improve** decision making
- **Express** risk in business terms
- **Improve** conversation on factors influencing risk
- **Tailored** to our business

Copyright 2019 FAIR Institute, Inc.

Joey's Tips for Effective Risk Management

FAIR CONFERENCE 2019

- **Understand** and **EMBRACE** risk holistically
- Ensure **high level alignment** with the overall business risk appetite - beyond IT/Infosec
- **Deliver risk metrics** that drive organizational discussion & decision
- Have **CISO and security leadership participation** in organizational growth strategy in a proactive manner
- Leverage **security as business enabler** and driver of operational efficiency
- Ensure **board level reporting drives cohesion and alignment** amongst C-Suite, not divisiveness
- Ensure IT and Security **strategic investments are balanced** against the Strategic/Tactical/Maturity readiness spectrum