# **The Human Factor:**
# Quantifying Human Risk

**Sara Anstey**

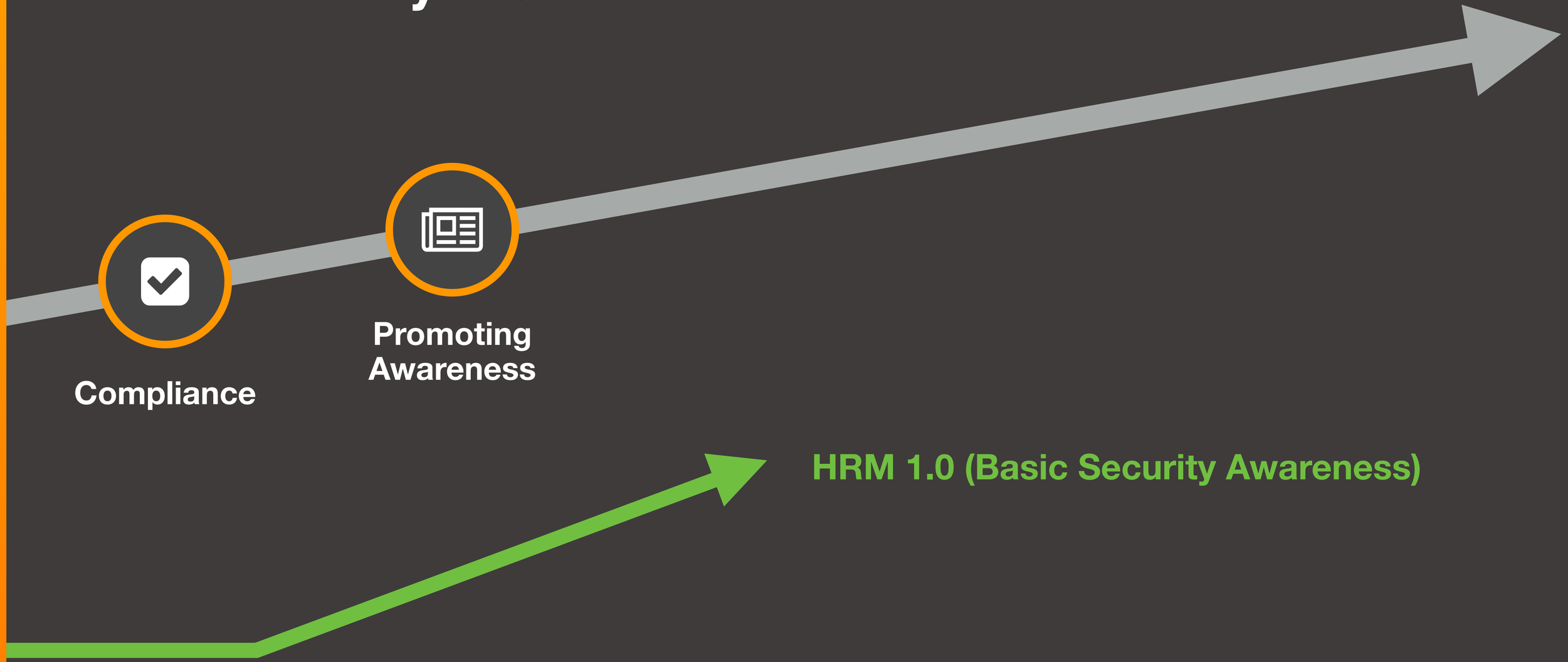
Novacoast - Director, Data Analytics and Risk

novacoast

# Human Risk Management

**Strategy for identifying, reporting on, and responding to human-caused risks in an organization**

# HRM Maturity Model



# Human Risk Quantification

# Risk

?

# Quantification

# The **Analysis Placebo**

| | Negligible **(<$10K)** | Minor **($10K-$100K)** | Moderate **($100K-$1M)** | Critical **($1M-$10M)** | Catastrophic **(>$10M)** |
|---|---|---|---|---|---|
| Frequent (99%+) | Medium | Medium | High | High | High |
| Likely (51%-98%) | Medium | Medium | Medium | High | High |
| Occasional (26%-50%) | Low | Medium | Medium | Medium | High |
| Seldom (1%-25%) | Low | Low | Medium | Medium | Medium |
| Improbable (<1%) | Low | Low | Low | Medium | Medium |

# The **Analysis Placebo**

**Risk A:** Likelihood ***50%***; Impact ***$9 million***
Expected loss $4.5 million **Medium**

**Risk B:** Likelihood ***60%***; Impact ***$2 million***
Expected loss $1.2 million **High**

| | Negligible **(<$10K)** | Minor **($10K-$100K)** | Moderate **($100K-$1M)** | Critical **($1M-$10M)** | Catastrophic **(>$10M)** |
|---|---|---|---|---|---|
| Frequent (99%+) | Medium | Medium | High | High | High |
| Likely (51%-98%) | Medium | Medium | Medium | High | High |
| Occasional (26%-50%) | Low | Medium | Medium | Medium | High |
| Seldom (1%-25%) | Low | Low | Medium | Medium | Medium |
| Improbable (<1%) | Low | Low | Low | Medium | Medium |

# Human

# The **Towel Debate**

# The **Towel Debate**

"75% of guests in this hotel reuse their towels"

"75% of guests in this room reuse their towels"

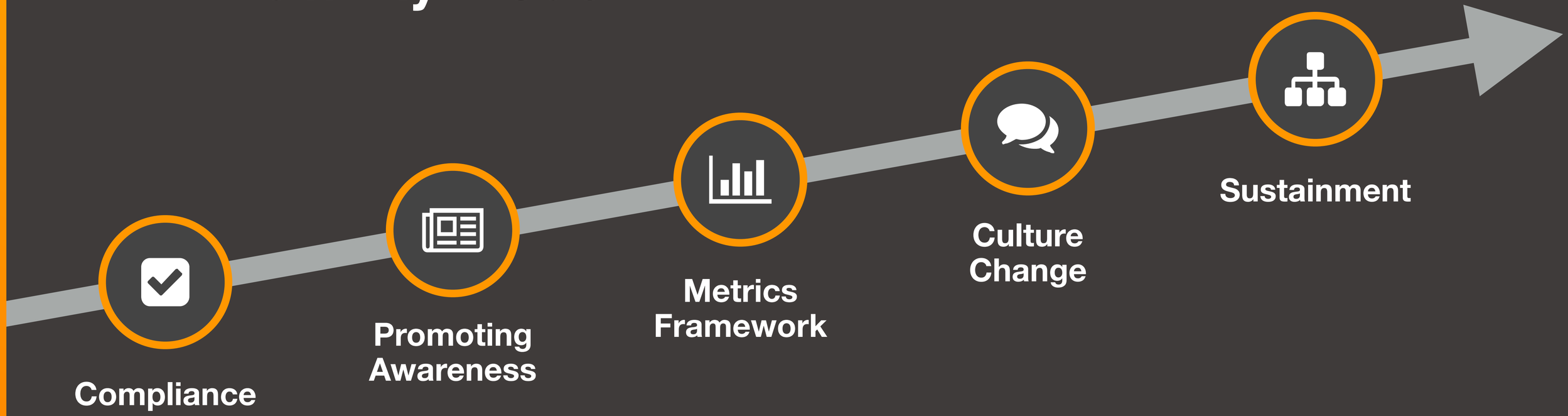
# The **Towel Debate**

**1** vs **1.6**

Room Hotel

# Human Risk Quantification

# HRM Maturity Model




HRM 1.0 (Basic Security Awareness)

Human Risk Management 2.0

# Expanding our view of security behaviors

## Web and endpoint security

- Attempts to install unauthorized software
- Attempts to access dangerous websites
- Mobile device updates
- Detection of malware

## Phishing and email security

- Phishing simulations: User actions for clicks, data entry, attachments
- Real phishing: User clicking and reporting actions on real phishing emails
- Real phishing: Detection of malware from email links and attachments

## Data loss & privacy security

- Attempts to send plain text passwords to personal email
- Detection of policy violations
- Blocks of share site uploads/downloads

## Security training

- Status of annual compliance training
- Status of new hire training
- Status of assigned training
- Phishing School
- Security training for risk mitigation actions

## Access and authentication account compromise

- Self-Service password resets
- Risky logins

# Humans Aren’t Optimal

# Thank **You**

“75% of the people in this room will connect with me on Linkedin”


Email: sanstey@novacoast.com

www.linkedin.com/in/sara-anstey

**Sara Anstey**

Novacoast - Director, Data Analytics and Risk