

# บันทึกกัปตัน: การนำทางฝ่าวิกฤตความเสี่ยง

ศิลปะและวิทยาศาสตร์ของการประเมินและบริหารความเสี่ยงระดับองค์กร  
(Risk Assessment & Management)

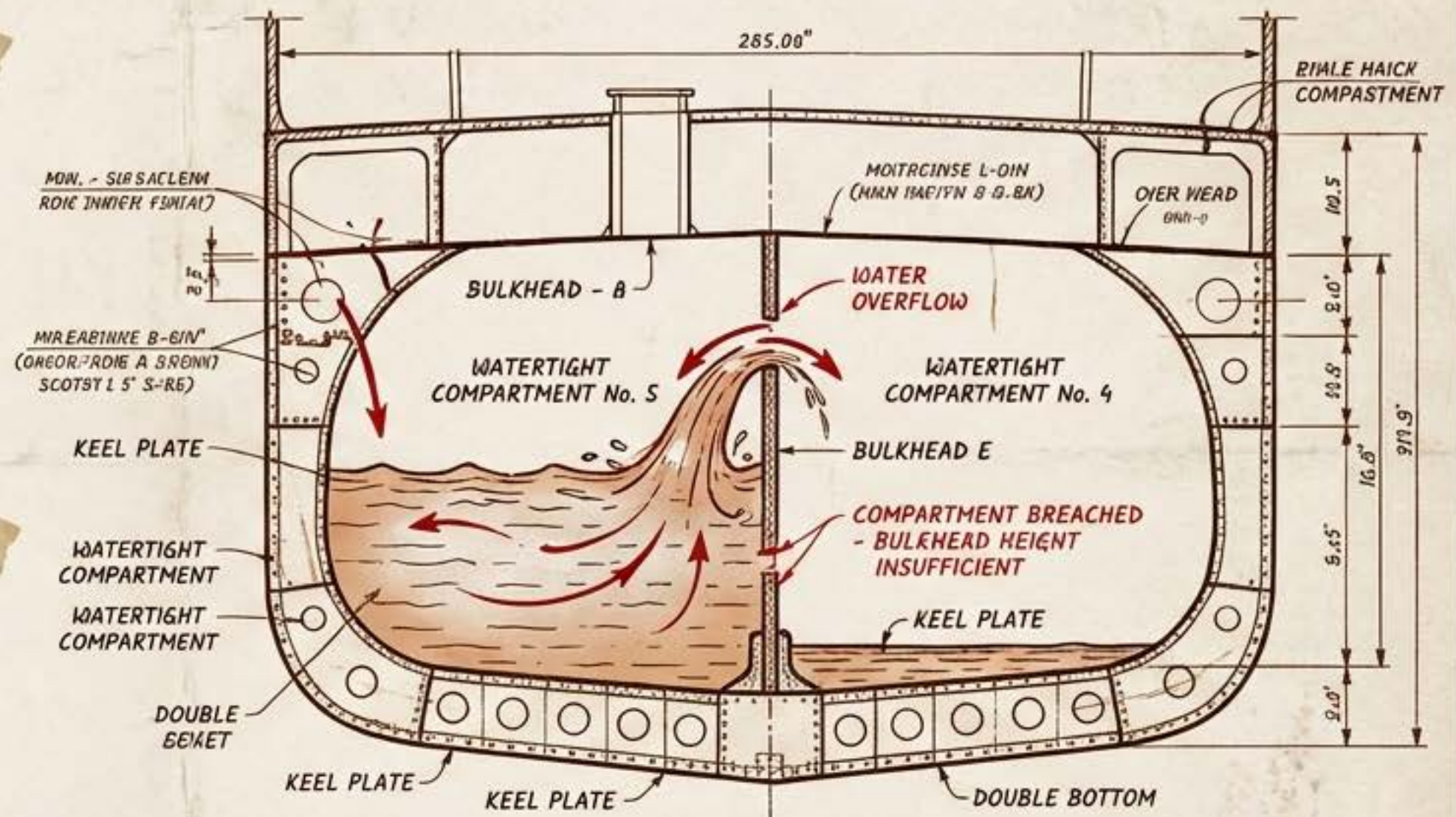


# ภาพลวงตาของระบบที่ "ไม่มีวันจบ"

# ข่าวเด่น

เดินเรือด้วยความเร็ว 22.5 น็อต  
ท่ามกลางคำเตือนภูเขาน้ำแข็ง 6-7 ครั้ง  
ผู้นำเชื่อมั่นในเทคโนโลยีและอดีตที่สำเร็จ  
(Historical Precedent Fallacy)

มีเวลาตัดสินใจเพียง 40 วินาที  
เรือชูชีพไม่เพียงพอ  
นำไปสู่การสูญเสียน่า 1,500 ชีวิต



# TELEGRAM

หายน่ะไม่ได้เกิดจากภูเขาน้ำแข็ง แต่เกิดจากการบริหารความเสี่ยงด้วยความเชื่อและอารมณ์  
มากกว่าหลักฐานเชิงประจักษ์

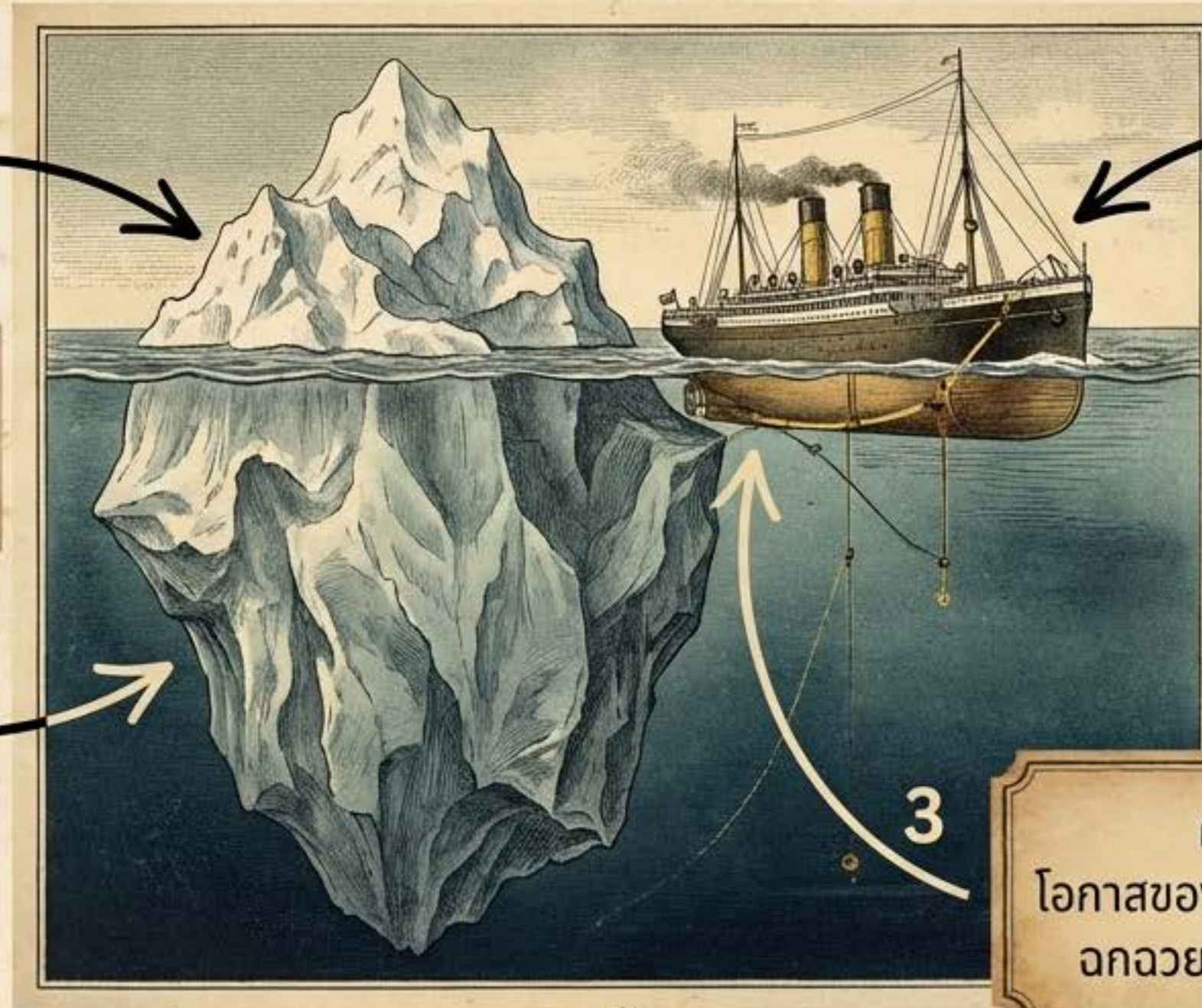
# พายุลูกใหม่ในศตวรรษที่ 21: จากแอตแลนติกสู่หาดใหญ่

**หาดใหญ่ (พ.ย. 2025):**  
ฝนตก 630 มม. ใน 72 ชม.  
(เหตุการณ์รอบ 300 ปี)  
โครงสร้างพื้นฐานล้มเหลว  
นำไปสู่ผู้เสียชีวิต 145+ คน

**ภัยไซเบอร์ (H1 2025):**  
ภัยคุกคามทางไซเบอร์ในไทยพุ่ง  
223,700 ครั้ง  
เชิร์ฟเวอร์กว่า 200,000  
เครื่องตกอยู่ในความเสี่ยง

ผู้นำยึดติดกับ "ข้อมูลในอดีต"  
(Past Precedent Fallacy)  
และโครงสร้างการสั่งการที่ซับซ้อน  
ทำให้ระบบที่เคยล้าสมัยกลายเป็นกรงขังเมื่อวิกฤตมาเยือน

# กายวิภาคของอันตราย: นิยามศัพท์พื้นฐาน



**ภัยคุกคาม (Threat):**  
สิ่งที่อยู่นอกเหนือการควบคุม  
(เช่น พายุ, แฮกเกอร์, ภูเขาไฟ)

**ความเปราะบาง (Vulnerability):**  
จุดอ่อนที่เราควบคุมและแก้ไขได้  
(เช่น ซอฟต์แวร์ไม่อัปเดต,  
วัฒนธรรมองค์กร, โครงสร้างเรือ)

**ความเสี่ยง (Risk):**  
โอกาสของความสูญเสียเมื่อภัยคุกคาม  
ฉกฉวยโอกาสจากความเปราะบาง

$$\text{Risk} = \text{Likelihood (โอกาสเกิด)} \times \text{Impact (ผลกระทบ)}$$

# เข็มนาฬิกาสำรวจ: กระบวนการประเมินความเสี่ยง

## วิเคราะห์ความเสี่ยง (Risk Analysis) -

นำข้อมูลมาคำนวณระดับความเสี่ยงเพื่อจัดลำดับความสำคัญ

## ระบุสินทรัพย์ (Asset ID) -

เราไม่สามารถป้องกันสิ่งที่เราไม่รู้ว่ามีอยู่ได้ (ข้อมูล, คน, ชื่อเสียง)

## ประเมินความเปราะบาง (Vulnerability Assessment) -

ค้นหาจุดอ่อนทางกายภาพ เทคนิค และวัฒนธรรมองค์กร

## ระบุภัยคุกคาม (Threat ID) -

สแกนหาศัตรู ทั้งภัยธรรมชาติ ภัยจากมนุษย์ และทางเทคนิค

# แผนที่เดินเรือ: การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative)

## สีแดง (Extreme):

ต้องหยุดการทำงานหรือแก้ไขทันที  
(เช่น น้ำท่วมเมืองหาดใหญ่)

## สีส้ม (High):

ต้องมีมาตรการจัดการเร่งด่วน

## สีเหลือง (Medium):

ยอมรับได้ชั่วคราวแต่ต้องมี  
แผนลดความเสี่ยง

## สีเขียว (Low):

ยอมรับได้และเฝ้าระวัง



# วิศวกรรมแห่งความปลอดภัย: เทคนิคโบว์ไท (Bow-Tie Analysis)



# ก้าวข้าม "ความเกรงใจ": การตั้งภูมิปัญญาด้วยเทคนิค Delphi

1

The Cultural Vulnerability:  
วัฒนธรรม "ความเกรงใจ"  
ทำให้พนักงานระดับล่างไม่กล้ารายงาน  
ความผิดปกติ ปิดกั้นข้อมูลความเสี่ยงที่  
สำคัญ (Risk Communication Failure)

2

The Delphi Solution:  
กระบวนการระดมสมองแบบ "นิรนาม"  
(Anonymous) และเป็นขั้นตอน

3

Result: ขจัดอคติจากการคล้อยตามกลุ่ม  
(Groupthink) และลดแรงกดดันทางสังคม  
ทำให้ได้ฉันทามติที่สะท้อนความเสี่ยงที่แท้จริง

## บัญชีแห่งความสูญเสีย: การวิเคราะห์เชิงปริมาณ (Quantitative Analysis)

Formula 1: ALE (ความสูญเสียคาดการณ์ต่อปี) = SLE (มูลค่าความเสียหายต่อครั้ง)  $\times$  ARO (อัตราความถี่ต่อปี)

Formula 2: ROSI = [(ALE ก่อนลงทุน - ALE หลังลงทุน - ต้นทุน) / ต้นทุน]  $\times$  100%

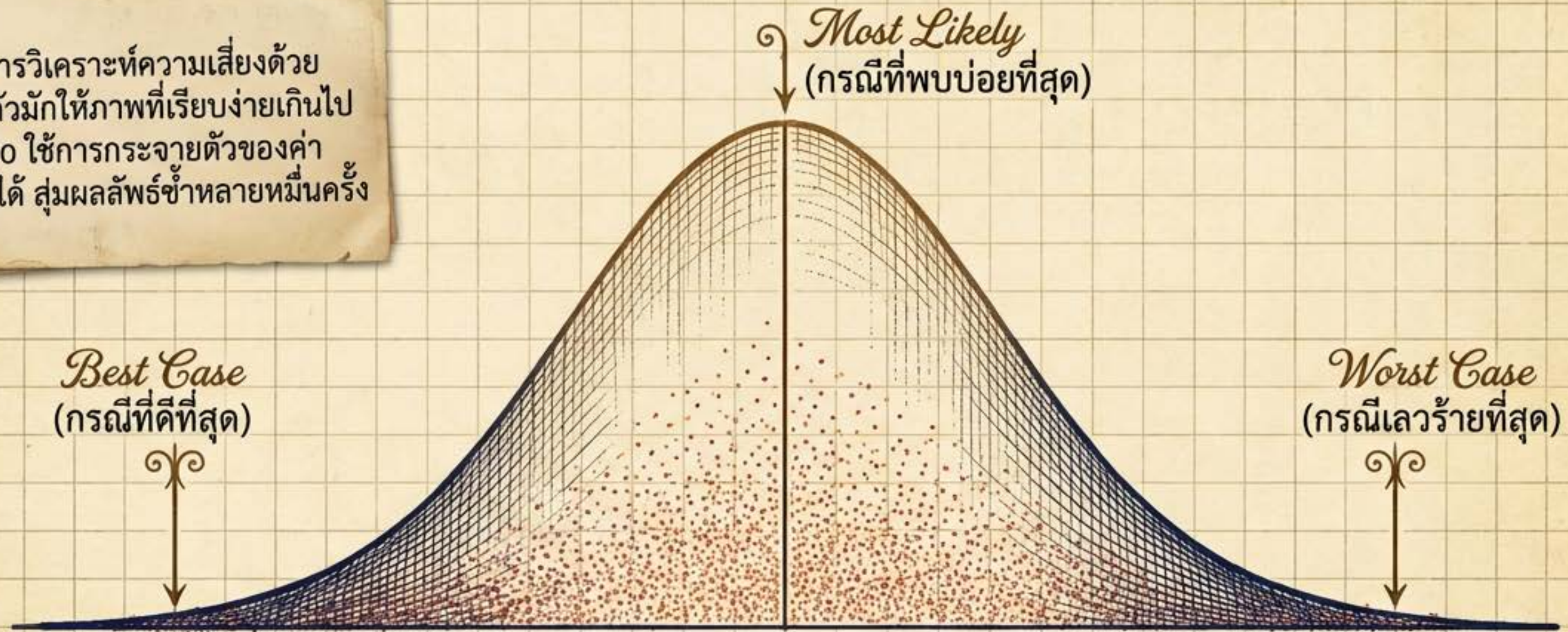
### Case Study:

|                             |                |
|-----------------------------|----------------|
| ความสูญเสียจาก Ransomware:  | 1.2 ล้านบาท/ปี |
| ลงทุน Firewall:             | 500,000 บาท    |
| ผลตอบแทนความปลอดภัย (ROSI): | 260%           |

เปลี่ยนค่าใช้จ่ายเป็นการลงทุน

# โอบรับความไม่แน่นอน: การจำลองสถานการณ์ Monte Carlo

Concept: การวิเคราะห์ความเสี่ยงด้วย  
ค่าคงที่ตายตัวมักให้ภาพที่เรียบง่ายเกินไป  
Monte Carlo ใช้การกระจายตัวของค่า  
ความเป็นไปได้ สุ่มผลลัพธ์ซ้ำหลายหมื่นครั้ง



ช่วยตอบคำถามว่า "ความเสี่ยงที่ความสูญเสียจะเกินขีดจำกัดที่รับได้ มีสูงแค่ไหน?"

คำสั่งจากห้องกัปตัน:  
กลยุทธ์การจัดการความเสี่ยง (The 4Ts)



**หลีกเลี่ยง**  
(Avoid / Terminate):  
ยกเลิกกิจกรรมที่ก่อให้เกิด  
ความเสี่ยง  
(เช่น ไม่สร้างบ้านในพื้นที่รับน้ำ)



**ลดความเสี่ยง**  
(Reduce / Treat):  
การติดตั้งมาตรการป้องกัน  
เพื่อลดโอกาสหรือผลกระทบ  
(เช่น ระบบ MFA, กล้อง CCTV)



**โอนย้าย**  
(Transfer / Share):  
ผลการผลกระทบทางการเงิน  
(เช่น ซื้อประกันภัยไซเบอร์)  
\*ข้อควรระวัง: โอนความรับผิดชอบ  
ทางกฎหมายและชื่อเสียงไม่ได้\*



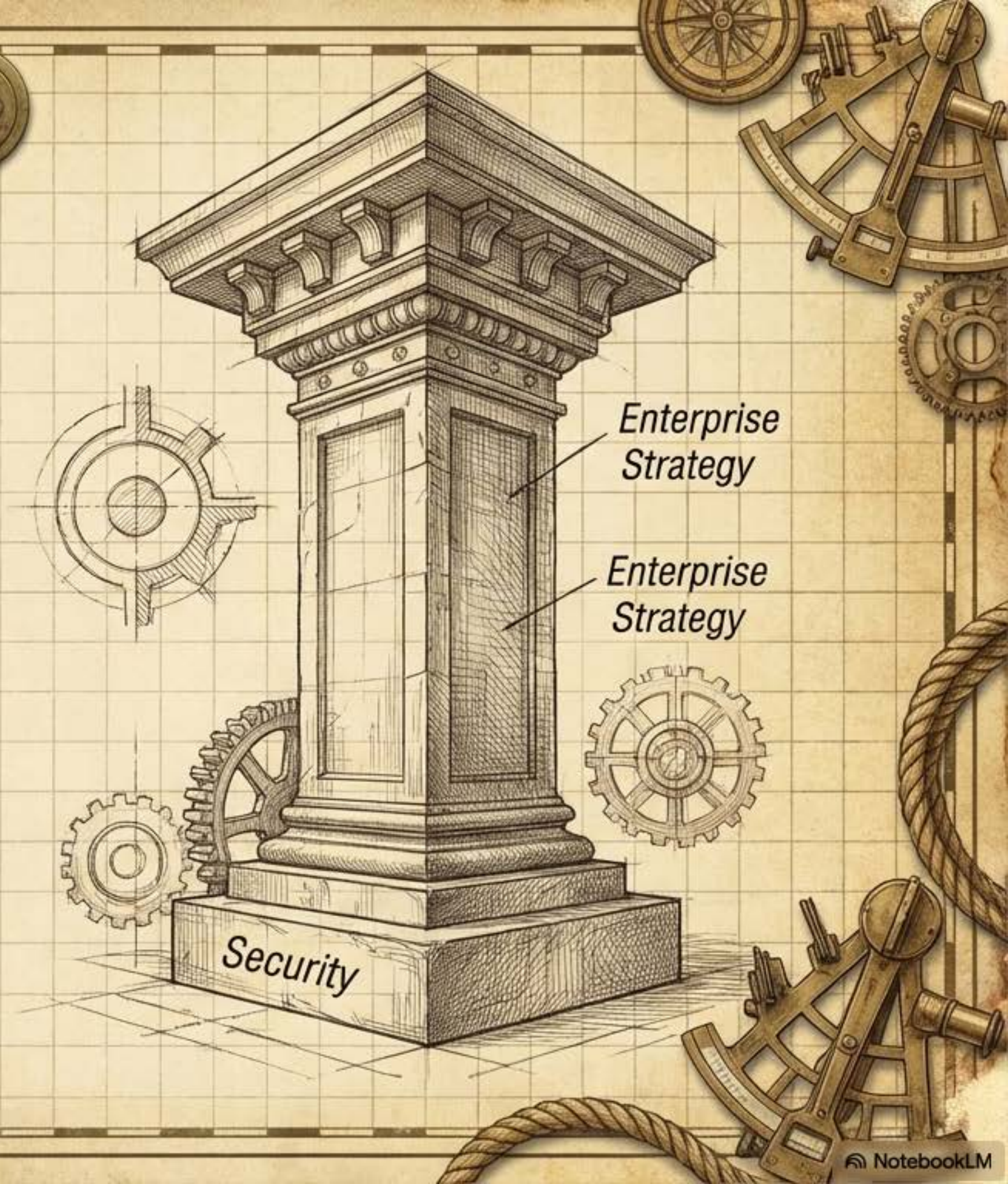
**ยอมรับ**  
(Accept / Tolerate):  
ตัดสินใจอย่างมีสติที่จะรับ  
ความเสี่ยงที่อยู่ในระดับ  
ที่ยอมรับได้

# บูรณาการทั้งกองเรือ: การบริหารความเสี่ยงระดับองค์กร (ERM)

The Frameworks (COSO 2017 & ISO 31000):  
ความปลอดภัยต้องสอดคล้องกับกลยุทธ์หลัก  
และวัฒนธรรมองค์กร

The Reality:  
ความมั่นคงปลอดภัยไม่ใช่แค่หน้าที่ของฝ่าย IT หรือ สปก.

Legal Stakes:  
ภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA)  
การละเลยการประเมินความเสี่ยงอาจนำไปสู่โทษปรับ  
สูงสุด 5 ล้านบาท และความรับผิดชอบส่วนบุคคล  
ของกรรมการบริษัท (Directors' Liability))



16/19/20

PSYCHOLOGICAL EVALUATION

Best Name: Thompson

Date: 18/9/2025

Detest: Lantheant

Appesence: David Houlder

EVALUATION RECORD

CONFIDENTIAL

EDGE LOBS OF ENCLORICAL BRIDGE: CONFIDENTIAL

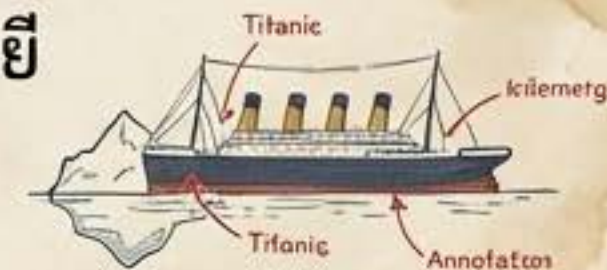
CONFIDENTIAL

# จุดอ่อนที่ซ่อนเร้น: อคติและพฤติกรรมมนุษย์ (Cognitive Biases)

Normalization of Deviance (ความคุ้นชินกับความผิดปกติ):  
การทำผิดเล็กๆ น้อยๆ จนชินชาและคิดว่าไม่เป็นไร  
(เช่น การเพิกเฉยต่อสัญญาณเตือนน้ำท่วม  
หรือการลดขั้นตอนความปลอดภัย)



Optimism Bias (การมองโลกในแง่ดีเกินไป):  
คิดว่า "ภัยพิบัติคงไม่เกิดกับเรา" หรือมั่นใจในเทคโนโลยี  
เกินความจริง (เช่น กรณีเรือไททานิก)



CLASSIFIED

The Core Issue: "มนุษย์" คือช่องโหว่ (Vulnerability)  
ที่อันตรายที่สุด หากขาดวัฒนธรรมองค์กรที่กล้าตั้งคำถาม

TOP SECRET

## บทสรุป: การสร้างเรือที่ยืดหยุ่น (The Resilient Ship)

เราไม่สามารถสร้างระบบที่ "ไม่มีวันจม"  
เพราะระบบเช่นนั้นไม่มีอยู่จริง

- ⚓ การบริหารความเสี่ยงไม่ใช่การพยายาม  
ทำให้ความเสี่ยงเป็นศูนย์ (Zero Risk)
- ⚓ หน้าทีของผู้นำคือการเป็นกัปตันที่มีวิสัยทัศน์  
รับฟังสัญญาณเตือน และเตรียมความพร้อม
- ⚓ เปลี่ยนภัยคุกคามที่ไม่แน่นอน  
ให้เป็นความเสี่ยงที่จัดการได้



ความแข็งแกร่งที่แท้จริง ไม่ใช่อยู่ที่การหลีกเลี่ยงพายุ  
แต่อยู่ที่ความพร้อมในการเผชิญหน้าและฟื้นตัวอย่างรวดเร็ว