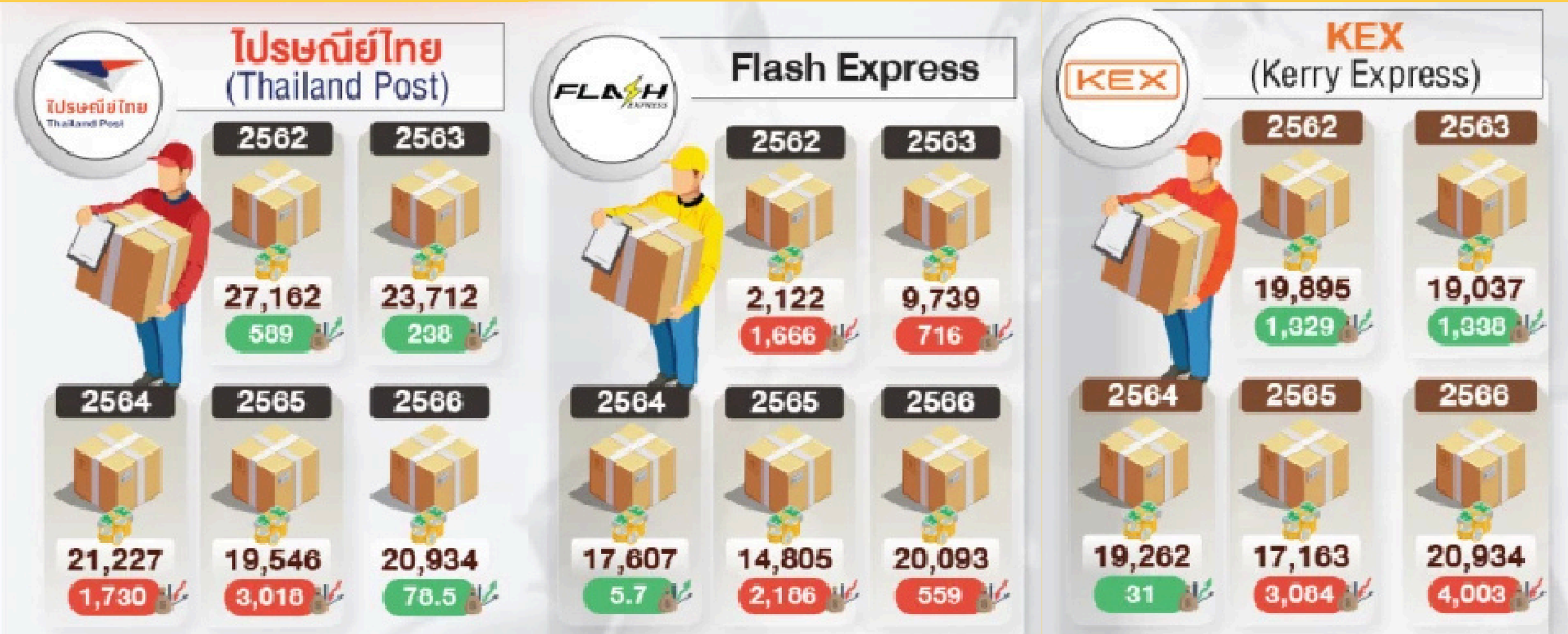

RISK MANAGEMENT
สงครามส่งด่วน

MYSURACHET.COM

RISK MANAGEMENT
สงครามส่งด่วน

สงครามส่งด่วน
MARKET SHARE



สงครามส่งด่วน
MARKET SHARE

MYSURACHET.COM

สงครามส่งด่วน
DIVERSIFICATION

MYSURACHET.COM

Flash Express

ดูแลการขนส่ง

Flash Fulfillment

ช่วยดูแลสต็อกสินค้า

Flashpay

ดูแลระบบจ่ายเงิน

Flash Money

ระบบยืมเงิน

MYSURACHET.COM

Security and Risk Management (Part2)

Instructor :
Surachet Suchaiya
PhD. Innovation MGT

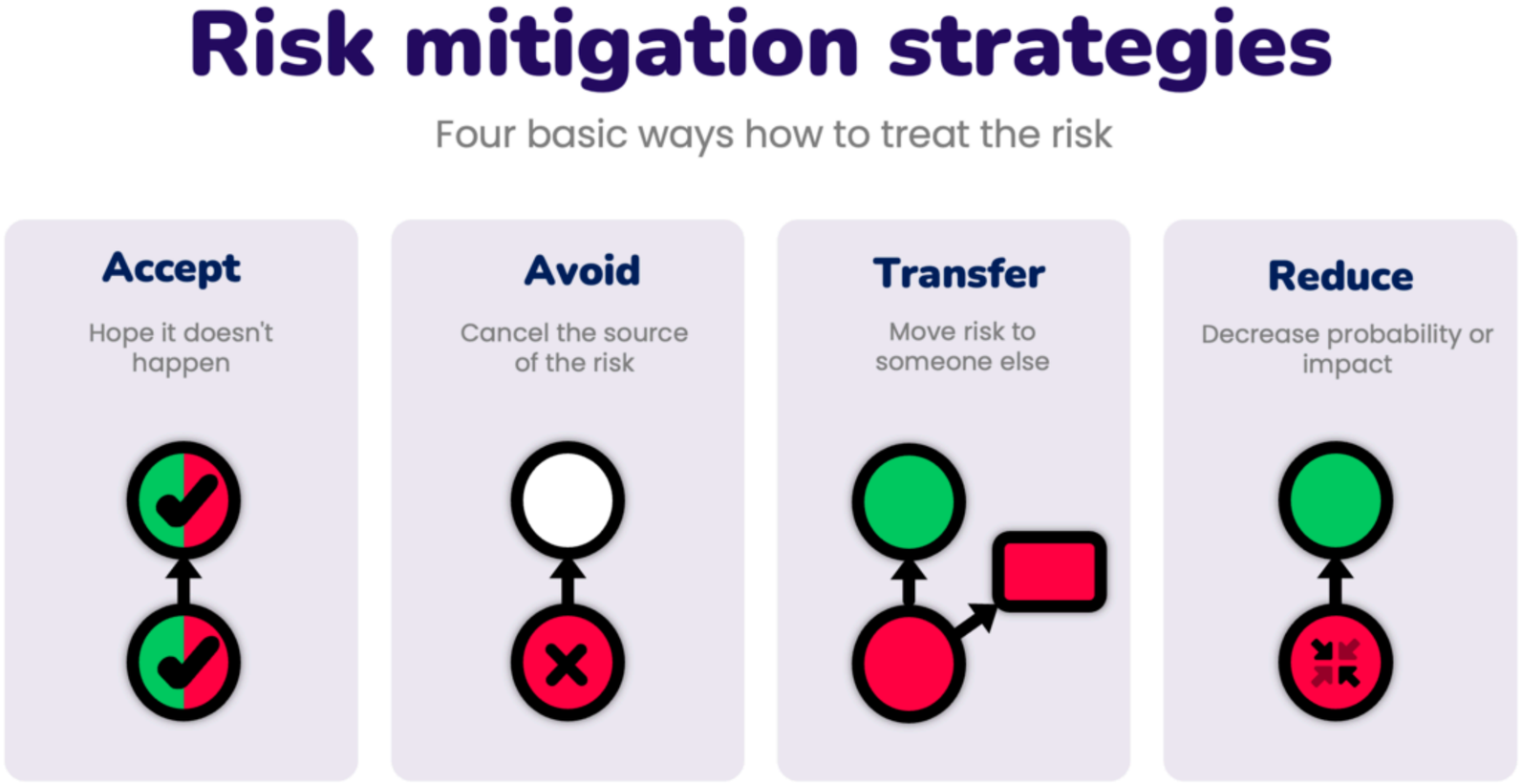
www.MySurachet.com

Risk Management Strategies

MYSURACHET.COM

แนวทางในการจัดการความเสี่ยง

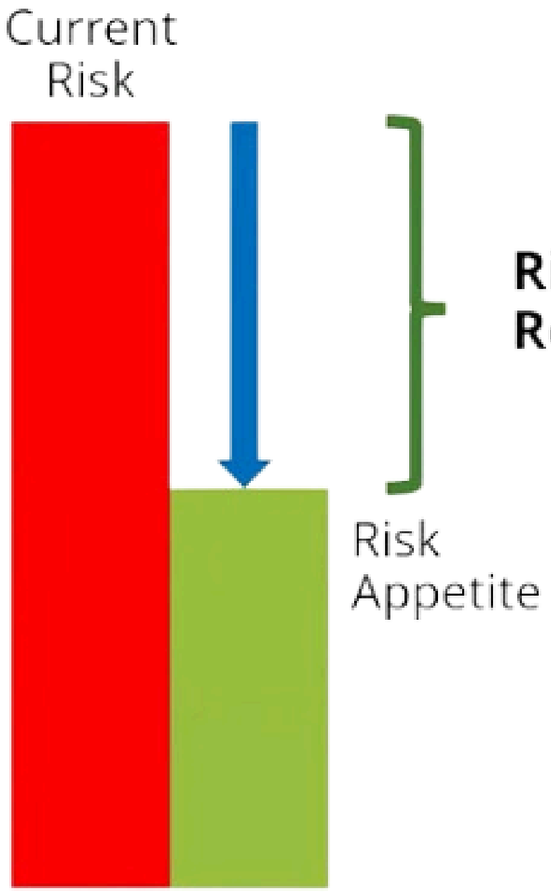
- การพัฒนาแผนตอบสนองต่อเหตุการณ์เพื่อเตรียมพร้อมสำหรับภัยคุกคาม



Goal of Risk Management

MYSURACHET.COM

To reduce the risk to an acceptable level while still able to pursue business objectives



Risk Response

- Avoidance
- Transfer
- Mitigate → Controls
- Acceptance

Ugly truths about controls:
- Control COSTS (i.e., control is not free)
- Control may fail = Control Risk

Risk Assessment Process

MYSURACHET.COM

Step :

1. Identify assets, threats, Vulnerabilities.

2.Analyze impact and likelihood.

3.Prioritize risks.

Risk = Threat x Vulnerabilities x Asset Value

Quatitative Risk Assessment

MYSURACHET.COM

AV: Asset Value

EF: Exposure Factor

SLE: Single Loss Expectancy

ARO: Annual Rate of Occurrence

ALE: Annualised Loss Expectancy

$$SLE = AV \times EF$$

$$ALE = SLE \times ARO$$

- Suitable for tangible/financial impact
- Need a reliable and sufficient amount of data
- Past statistics can be helpful
- Can be less subjective

Quatitative Risk Assessment

MYSURACHET.COM

- Building on land = 1,000,000 THB
- 1 Fire incident will destroy 70% of the building on land (เช่น ฐากรากยังอยู่ ที่ดินยังอยู่ แต่ตึกไฟไหม้หมด)
- Fire incident will occur once every 20 years

1. Find AV, EF, ARO
2. Calculate SLE, ALE

Quatitative Risk Assessment

MYSURACHET.COM

- Building on land = 1,000,000 THB
- 1 Fire incident will destroy 70% of the building on land (เช่น ฐากรากยังอยู่ ที่ดินยังอยู่ แต่ตึกไฟไหม้หมด)
- Fire incident will occur once every 20 years

AV

EF

ARO = 1/20 = 0.05 = 5%

1. Find AV, EF, ARO
2. Calculate SLE, ALE

SLE = 1,000,000 * 70% = 700,000 THB

Quatitative Risk Assessment

MYSURACHET.COM

- Building on land = 1,000,000 THB
- 1 Fire incident will destroy 70% of the building on land (เช่น ฐากรากยังอยู่ ที่ดินยังอยู่ แต่ตึกไฟไหม้หมด)
- Fire incident will occur once every 20 years

AV

EF

ARO = 1/20 = 0.05 = 5%

1. Find AV, EF, ARO
2. Calculate SLE, ALE

SLE = 1,000,000 * 70% = 700,000 THB

ALE = 700,000 * 5% = 35,000 THB

Qualitative Risk Assessment

MYSURACHET.COM

- Suitable for intangible aspects, e.g., reputation risk
- Consider both probability and impact
- Can be subjective
- Sometimes is the best option if the sufficient or precise data is not available

Risk Monitoring

Continuous Assessment: Adapts to evolving threats.

Example:

- Conducting quarterly vulnerability scans.
- Confirm organization change attribute those create new risk.

Compliance Requirement

Compliance Requirement

MYSURACHET.COM

- **Regulations :** GDPR, HIPAA, PCI-DSS
- **Importance :** Avoid penalties and legal repercussions

Things to note : PCI-DSS is not a part of law, just regulation create by private industry

Business Continuity Planning (BCP)

MYSURACHET.COM

- **Objective :** Ensure critical functions continue during disruptions.
- **Components :** Business Impact Analysis (BIA), recovery strategies.
- **Example :** BIA priotitizes customer support during outages.

Disaster Recovery Planning (DRP)

MYSURACHET.COM

- **Focus :** Restore IT Systems and data after a disaster.
- **Example :** Cloud-Based backups for repid recovery.

Personnel

Personnel Security Policies

MYSURACHET.COM

- **Objective :** Ensure employees understand security responsibilities.
- **Measures :** Background checks, security training.

Social Engineering

MYSURACHET.COM

- **Phishing :** email to steal information or install malware on user systems.
- **Spear phising :** A more targeted form of phishing -> Target specific group of people or department.
- **Business E-Mail Compromise (BEC) :** Convicing receiver to transfer funds or pay invoice.
- **Whaling :** Phishing that targets high-value or high-ranking individual.

Social Engineering (2)

MYSURACHET.COM

- **Smishing :** Phising via SMS or instant messaging.
- **Vishing :** Voice-based phishing, e.g., via mobile phone or VOIP Service.
- **Shoulder surfing :** Watch the person typing or their monitor display.
- **Hox :** Convince target to perform an action that will cause problem/reduce their IT Security.

Security Awareness Training

MYSURACHET.COM

An effective cure against social engineering attack

- **Goal :** Educates staff on security best practices.
- **Topics :** Phishing drill, password management, incident reporting.
- **Example :** Conducting phishing simulation exercises.

MYSURACHET.COM

Introduction to Data and Information Protection

Data Classification

MYSURACHET.COM

- **Purpose :** Catagorize Databased on sensitivity.
- **Level :** Public, Internal, Confidential, Secret, TopSecret.
- **Approaches :**
  - Manual Classification : employees label data during creation.
  - Automated Classification : Tools use metadat and content analysis.
- **Example :** Making financial records as ‘Confidential’ in CRM.

Information Lifecycle Management

- **Creation :** Data is securely generated or acquired.
- **Storage :** Securely stored in databases, backups.
- **Use :** Secure utilization of data in operations.
- **Share :** Securely send and receive information.
- **Achiving** : Secure Long-term preservation of historical data.
- **Destruction** : Secure deletion or shredding.

Privacy Priciples and Data Protection

- **Transparency :** inform users how data will be used.
- **Consent :** Obtain permission for data collection and processing.
- **Data Minimization :** Collect only what is necessary.
- **Purpose Limitation :** Use data only for specified objectives.

Regulatory context : GDPR, PDPA.

Example : Requiring explicit opt-in for email marketing.

Workshop


TRAINING
GOAL
IDEA
SKILLS
WORKSHOP
TEAM
PRACTICE
RESULTS
TREND

Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม 1 : การประเมินและการจัดการความเสี่ยง

วิเคราะห์องค์กรสมมติ และดำเนินการประเมินความเสี่ยงโดยใช้สูตร

ความเสี่ยง = ภัยคุกคาม × ช่องโหว่ × มูลค่าทรัพย์สิน

ระบุ: 1.ทรัพย์สินสำคัญ, 2.ภัยคุกคามหลัก, 3.ช่องโหว่

ให้จัดลำดับความเสี่ยงตามความสำคัญและเสนอแนวทางลดความเสี่ยง

เป้าหมาย: แสดงความเข้าใจในกระบวนการประเมินความเสี่ยงและความสามารถในการนำเสนอแนวทางจัดการที่เป็นรูปธรรม

Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม 2 : การวางแผนความต่อเนื่องทางธุรกิจ (BCP) และการกู้คืนระบบ (DRP)

จงพัฒนาแผนความต่อเนื่องทางธุรกิจ (BCP) และ แผนการกู้คืนระบบ (DRP) สำหรับองค์กรที่เผชิญการโจมตีทางไซเบอร์

เนื้อหาที่ต้องครอบคลุม:

1.การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA)

2.กลยุทธ์การฟื้นฟูสำหรับฟังก์ชันสำคัญ

3.ขั้นตอนการกู้คืนระบบ IT รวมถึงการใช้ระบบสำรองข้อมูลบนคลาวด์

เป้าหมาย: แสดงให้เห็นถึงการวางแผนจัดการระบบที่สำคัญขององค์กรเมื่อเกิดเหตุการณ์ไม่คาดฝัน

Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม 3 : การโจมตีทางวิศวกรรมสังคม (Social Engineering) และการฝึกอบรมความมั่นคงปลอดภัย

ให้ออกแบบแคมเปญสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยในองค์กรเพื่อลดความเสี่ยงจากการโจมตีทางวิศวกรรมสังคม

เนื้อหาที่ต้องครอบคลุม:

1.การฝึกซ้อมการโจมตีแบบฟิชชิ่ง (Phishing Simulation)

2.วิธีป้องกัน Spear Phishing, Smishing, และ Vishing

3.คำแนะนำเกี่ยวกับการจัดการรหัสผ่านและการรายงานเหตุการณ์

เป้าหมาย: แสดงให้เห็นถึงความสำคัญของการฝึกอบรมและการสร้างความตระหนักในองค์กรเพื่อลดช่องโหว่ด้านความมั่นคงปลอดภัย

Workshop

MYSURACHET.COM

กิจกรรมกลุ่ม 4 : การจัดประเภทข้อมูลและการจัดการวงจรชีวิตข้อมูล

ให้เสนอแนวทางการจัดประเภทข้อมูลในองค์กรการเงิน

เนื้อหาที่ต้องครอบคลุม:

1.การแบ่งประเภท เช่น Public, Confidential, Secret

2.วิธีการจัดประเภทข้อมูลแบบ Manual และ Automated

3.ขั้นตอนการจัดการวงจรชีวิตข้อมูล เช่น การสร้าง, การใช้, การทำลายอย่างปลอดภัย

เป้าหมาย: แสดงความสามารถในการจัดการข้อมูลอย่างปลอดภัยตลอดวงจรชีวิตของข้อมูล

MYSURACHET.COM

Thank You

Let’s Connect with Us!

www.MySurachet.com

Biz Card Contact