# บทที่ 2 รูปแบบของภัยคุกคาม อันตราย และการก่อการร้าย

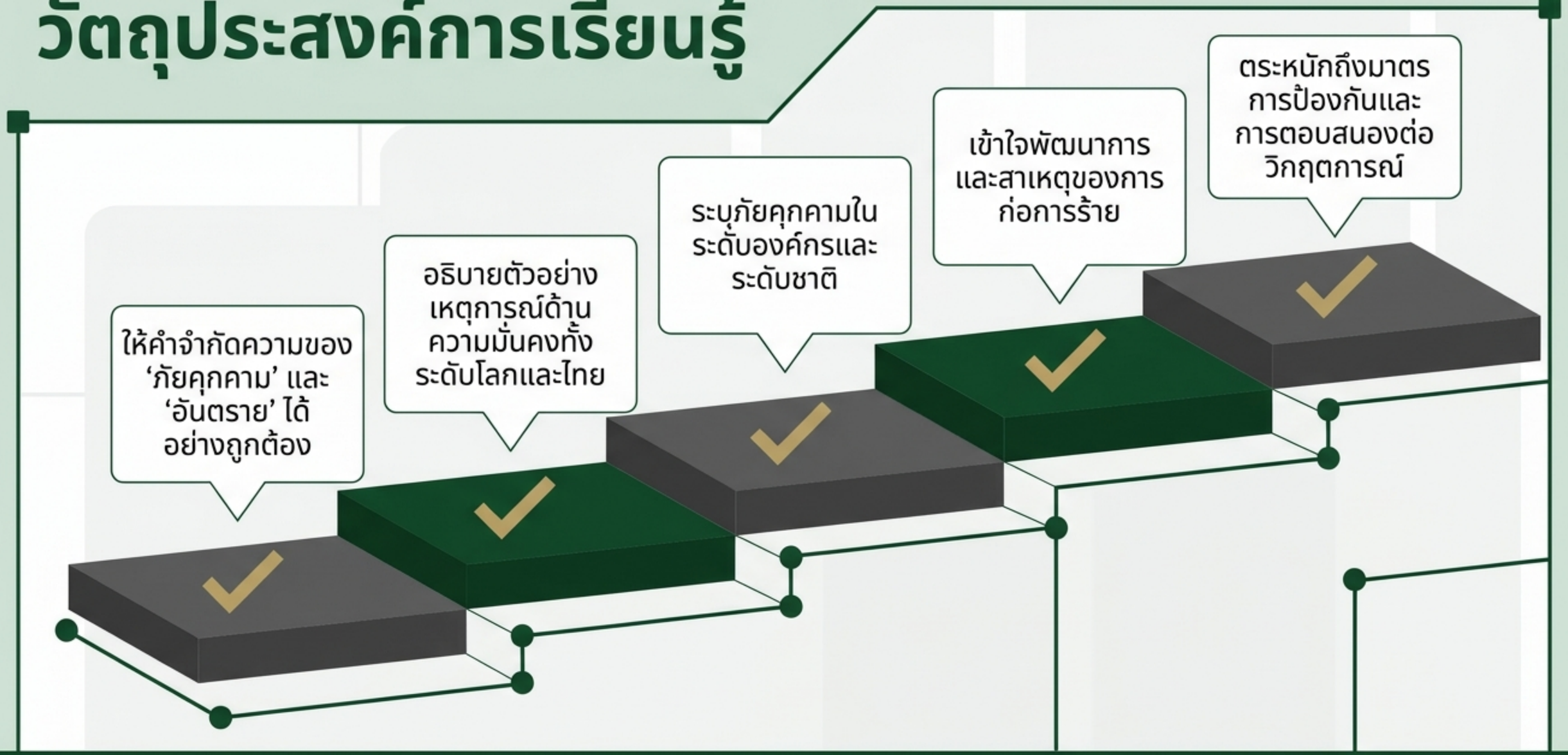
รายวิชา: SEM1201 การบริหารและการจัดการความมั่นคง

ผู้บรรยาย: ผศ.ดร.หทัยพันธน์ สุนทรพิพิธ

สาขาวิชา: การบริหารและการจัดการความมั่นคง

การจัดการความมั่นคงเริ่มต้นจากการทำความเข้าใจภัยคุกคาม

# วัตถุประสงค์การเรียนรู้




ความเข้าใจที่ถูกต้องคือรากฐานของการป้องกันที่มีประสิทธิภาพ

# ภาพรวมของภัยคุกคามและอันตรายในสังคมร่วมสมัย


เหตุการณ์ร้ายแรงนำมาซึ่งความสูญเสียมหาศาล

ภาครัฐและเอกชนต้องว่าจ้างผู้เชี่ยวชาญเพื่อบริหารจัดการ

การจัดการความกังวลและปกป้องสวัสดิภาพคือหัวใจของผู้จัดการความมั่นคง

# นิยามและข้อแตกต่าง: ภัยคุกคามและอันตราย

| องค์ประกอบ | ภัยคุกคาม (Threat) | อันตราย (Hazard) |
| --- | --- | --- |
| ลักษณะ | มีเจตนา (Intentional) | อุบัติเหตุ/ธรรมชาติ (Accidental/Natural) |
| แหล่งกำเนิด | พฤติกรรมมนุษย์ | สิ่งแวดล้อมหรือระบบล้มเหลว |
| นิยามหลัก | การแสดงเจตนาทำร้าย หรือสิ่งบ่งชี้ว่าอันตรายกำลังจะเกิด | แหล่งที่มาของความไม่ปลอดภัย หรือเหตุไม่คาดคิด |
| ตัวอย่าง | เหตุกราดยิง อาชญากรรม | น้ำท่วม แผ่นดินไหว |

**ภัยคุกคามมีเจตนาซ่อนเร้น แต่อันตรายคือเหตุแทรกซ้อนที่ไม่คาดคิด**

# ประเภทของอันตราย: ธรรมชาติและน้ำมือมนุษย์

## ภัยธรรมชาติ

1. แผ่นดินไหว พายุไต้ฝุ่น อุทกภัย

2. ปรากฏการณ์ที่ไม่รู้จักและคาดเดาไม่ได้

## ภัยจากมนุษย์และระบบ

1.อุบัติเหตุ: เครื่องปฏิกรณ์นิวเคลียร์ขัดข้อง, การระเบิดทางอุตสาหกรรม

2. กิจกรรมที่ควบคุมไม่ได้: การตัดไม้ทำลายป่า, จราจรหนาแน่น

**การเตรียมการล่วงหน้ามีประโยชน์สูงสุดต่อการรักษาความปลอดภัย (Purpura, 2010)**

**การวางแผนล่วงหน้าคือเครื่องมือเดียวในการรับมือกับความไม่แน่นอน**

# เหตุกราดยิง (Active Shooter) และการเตรียมพร้อม

## บริบทและกรณีศึกษา

- การพยายามฆ่าผู้อื่นในพื้นที่จำกัดหรือสาธารณะ
- กรณีสหรัฐฯ: Virginia Tech (2007), Pulse (2016), Las Vegas (2017)
- กรณีไทย: นครราชสีมา (พ.ศ. 2563)

**1. วิ่ง (Run):** หาทางออกทันที

**2. ซ่อน (Hide):** หากหนีไม่ได้ ให้ซ่อนตัวและเงียบ

**3. ต่อสู้ (Fight):** ทางเลือกสุดท้ายเพื่อเอาชีวิตรอด

**ในสถานการณ์กราดยิง ทุกวินาทีมีค่าอย่างยิ่ง**

# กรณีศึกษา: อุทกภัยครั้งใหญ่ของไทย ปี พ.ศ. 2554

**12.8 ล้าน**

ประชาชนที่ได้รับผลกระทบ

**813**

ผู้เสียชีวิต (ราย)

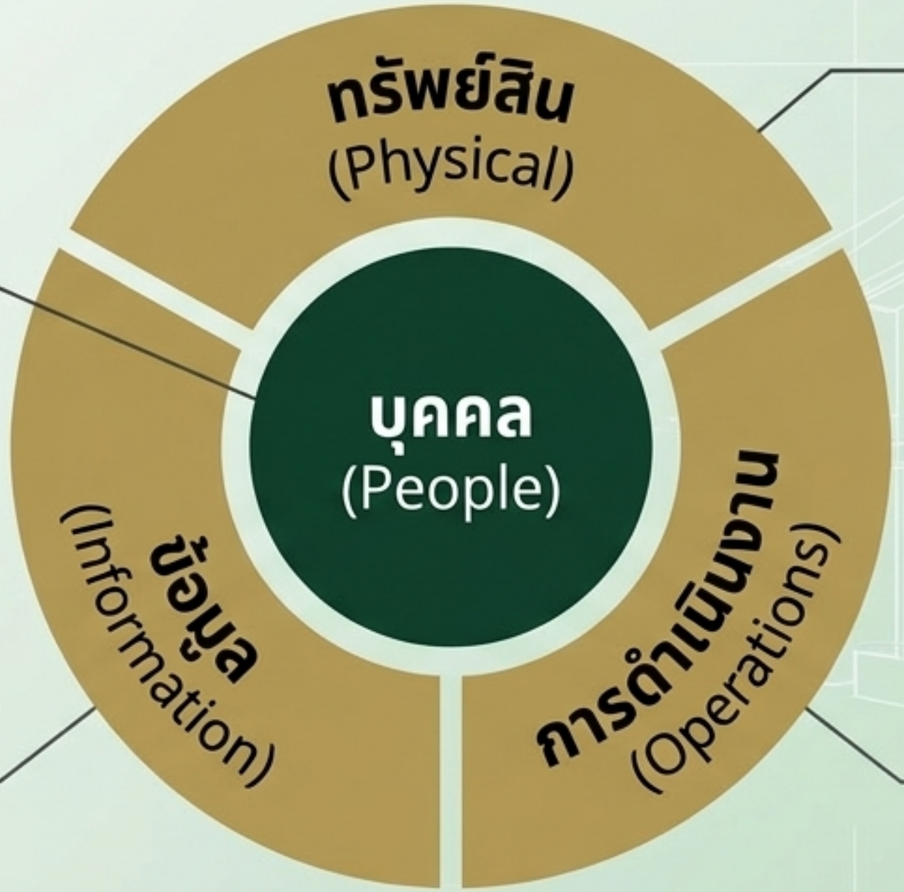
**1.44**

มูลค่าความเสียหาย (ล้านล้านบาท)

- ครอบคลุมพื้นที่กว่า 150 ล้านไร่
- บทเรียนสำคัญ: ความจำเป็นของแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และการจัดการความเสี่ยง

ภัยพิบัติทางธรรมชาติสามารถสร้างความสูญเสียเทียบเท่าวิกฤตเศรษฐกิจระดับชาติ

# การปกป้องบุคคล ทรัพย์สิน และการดำเนินงาน




อาคาร สินค้า
ยานพาหนะ เงินสด

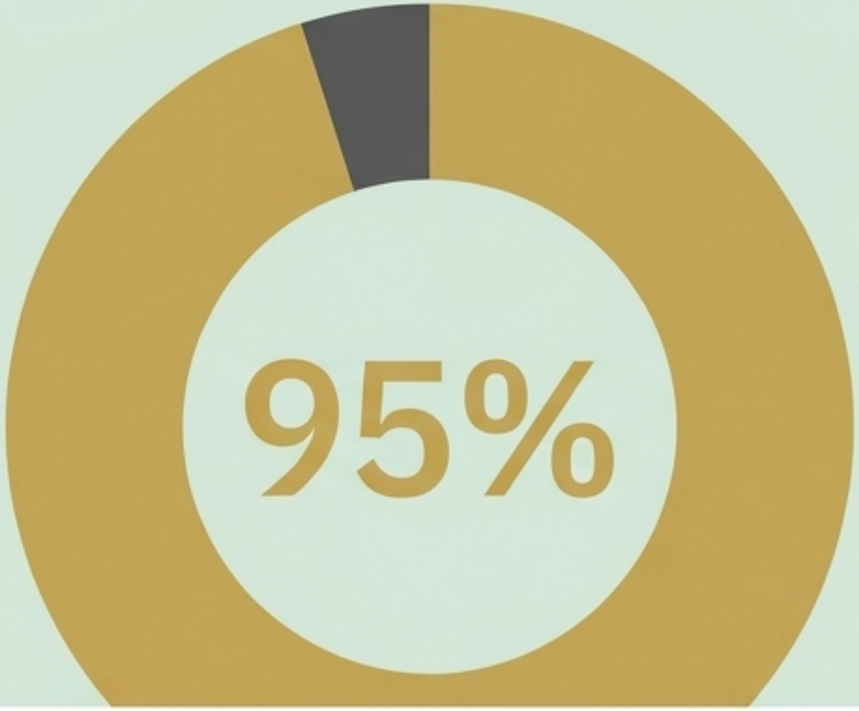
คุ้มครองชีวิตพนักงาน
ลูกค้า ผู้มาติดต่อ
(จัดอบรม, ฝึกซ้อมอพยพ)

ความลับองค์กร
ทรัพย์สินทางปัญญา

แผนสำรองกรณีไฟดับเพื่อ
รักษาระบบควบคุมอาคาร,
การปกป้องสิ่งแวดล้อม
จากกิจกรรมองค์กร

การรักษาความปลอดภัยครอบคลุมตั้งแต่ชีวิตพนักงานไปจนถึงชื่อเสียงองค์กร

# ภัยคุกคามภายใน: การโจรกรรมและการฉ้อโกง




ของธุรกิจในสหรัฐฯ ประสบปัญหาการโจรกรรมในที่ทำงาน (Weisbrot, 2021). 75% ของพนักงานยอมรับว่าเคยขโมยของนายจ้าง

## การโจรกรรม (Theft)

การขโมยสินค้า เงินสด ข้อมูล หรืออุปกรณ์ (ใช้เวลาเฉลี่ยเกือบ 2 ปีก่อนตรวจพบ)

## การฉ้อโกง (Fraud)

การหลอกลวงเพื่อผลประโยชน์ เช่น ตกแต่งบัญชีค่าใช้จ่าย หรือสร้างรายงานเท็จ

พนักงานที่ไม่ซื่อสัตย์คือผู้กระทำผิดหลักของการโจรกรรมภายในองค์กร

# กรณีศึกษาความล้มเหลวด้านความมั่นคงทางการเงิน

**Enron Corporation**
**เหตุการณ์:** ผู้บริหารตกแต่งบัญชีที่ฉ้อฉลเพื่อซ่อนหนี้ (Accounting Fraud)
**ผลลัพธ์** : ล้มละลายมูลค่า 63.4 พันล้านดอลลาร์ นักลงทุนสูญเงินออมเกษียณ

2001

2008

**บทเรียน:** องค์กรต้องมีความโปร่งใส และกระจายความเสี่ยงในการลงทุน (Purpura, 2010)

**Lehman Brothers**
**เหตุการณ์:** วิกฤตสินเชื่อซับไพรม์ (Subprime Crisis)
**ผลลัพธ์:** การยื่นล้มละลายที่ใหญ่ที่สุดในประวัติศาสตร์สหรัฐฯ

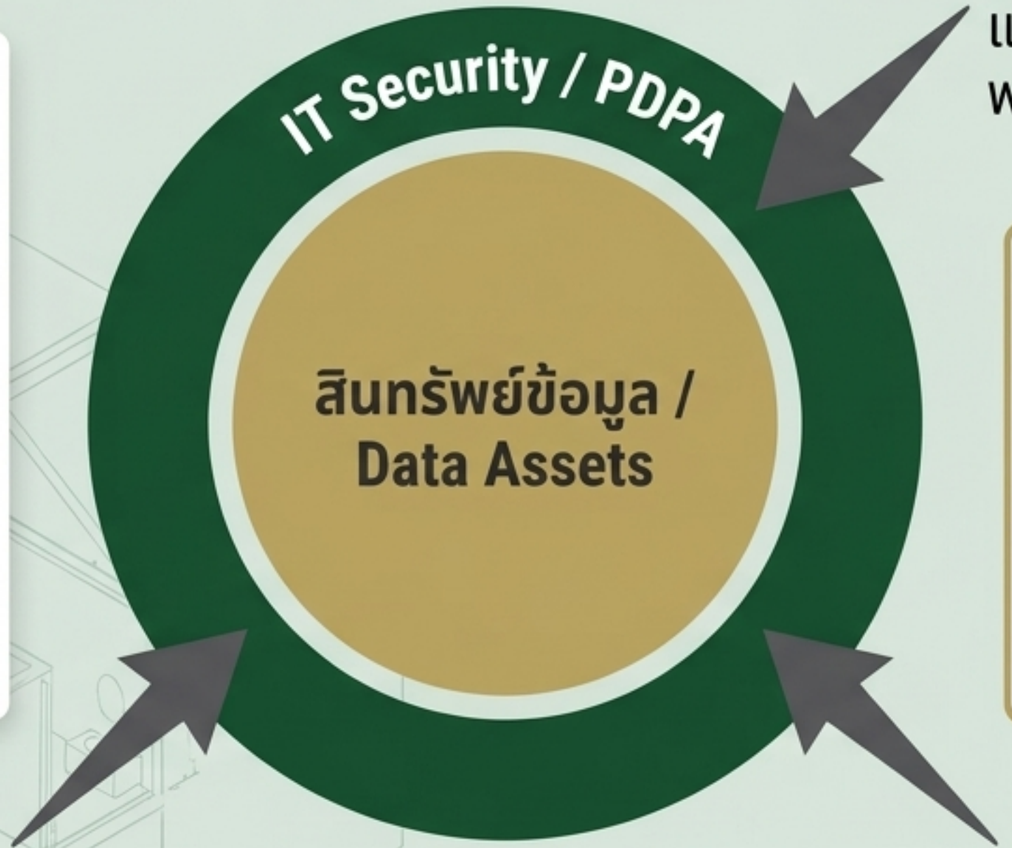
การขาดจริยธรรมทางการเงินคือภัยพิบัติที่สามารถทำลายองค์กรระดับโลกได้

# สินทรัพย์ข้อมูลและอาชญากรรมไซเบอร์

## Cyber Risk Architecture

**ความสำคัญ:** ธุรกิจยุคใหม่พึ่งพาข้อมูลลับ (สูตรลับ, ข้อมูลลูกค้า) เพื่อความอยู่รอด

**ข้อบังคับ:** พ.ร.บ. **คุ้มครองข้อมูลส่วนบุคคล** (PDPA) บังคับให้องค์กรต้องปกป้องข้อมูล




**ภัยคุกคาม (Cyber Threats):** แฮกเกอร์, สายลับอุตสาหกรรม, พนักงานภายใน

**กรณีศึกษา: Yahoo (2016)**

ข้อมูลผู้ใช้ 3 พันล้านบัญชีถูกขโมย นำไปสู่คดีความและค่าปรับเกือบ 150 ล้านดอลลาร์ (Chellani, 2020)

**ในยุคดิจิทัล ข้อมูลคือสินทรัพย์ที่มีค่าที่สุดและตกเป็นเป้าหมายมากที่สุด**

# อาชญากรรมข้ามชาติและการฟอกเงิน

Academic Blueprint of Security

**อาชญากรรมข้ามชาติ (Transnational Crime):**
การกระทำผิดที่มีพื้นที่มากกว่าหนึ่งประเทศ (Albanese, 2013)
เช่น ค้ามนุษย์ ขโมยข้อมูลบุคคล (Identity Theft) หลอกลวง (Phishing)

**ความท้าทาย:**
ผู้ก่อเหตุและเหยื่ออยู่คนละประเทศ ขัดขวางการสืบสวนบังคับใช้กฎหมาย

**การฟอกเงิน (Money Laundering):** เปลี่ยนเงินผิดกฎหมายให้ดูถูกกฎหมายผ่านธุรกิจบังหน้า (มักเป็นทุนก่อการร้าย)

**กฎหมายไทย:** พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ให้สถาบันการเงินรายงานธุรกรรมต้องสงสัย

**พรมแดนของรัฐไม่ใช่ขีดจำกัดสำหรับอาชญากรข้ามชาติ**

# การปกป้องแบรนด์และภัยพิบัติทางอุตสาหกรรม

**หลักการ: ‘แบรนด์’ คือสินทรัพย์และชื่อเสียงองค์กรที่ต้องได้รับการปกป้องอย่างยิ่งยวด**

## กรณีศึกษา: Exxon Valdez (1989)

- น้ำมันดิบรั่วไหล 10.8 ล้านแกลลอนในยอลาสก้า
- **ปัญหาหลัก:** การตอบสนองล่าช้า (Crisis Response Failure) ทำให้สูญเสียค่าชดเชยมหาศาล

## กรณีศึกษา: BP Deepwater Horizon (2010)

- ภัยพิบัติทางอุตสาหกรรมและสิ่งแวดล้อมครั้งใหญ่ที่สุด
- **ผลกระทบ:** ตั้งกองทุนชดเชยกว่า 2 **หมื่นล้านดอลลาร์**

**ชื่อเสียงที่สร้างมานานนับปี อาจพังทลายได้ในวันเดียวจากภัยพิบัติทางอุตสาหกรรม**

# สินค้าปลอมแปลงและการปนเปื้อนของผลิตภัณฑ์



## 1. ภัยคุกคาม (Threat)

- **สินค้าปลอม:** ยาปลอม 77% ในเออนไลน์ (Bell, 2019), อะไหล่รถยนต์
- **การปนเปื้อน:** เชื้อ E. coli (Jack in the Box, 1993), ไวรัสตับอักเสบเอ (Chi-Chi's, 2003)

## 2. ผลกระทบ (Consumer Harm)

- อันตรายต่อสุขภาพ การเจ็บป่วย และเสียชีวิต (Marcin, 2018)

## 3. ผลลัพธ์ (Business Destruction)

- คดีความ การจ่ายค่าชดเชย และการปิดกิจการถาวร

**ภัยคุกคามต่อความปลอดภัยของสินค้าคือภัยคุกคามต่อความอยู่รอดของธุรกิจ**

# ความหมายและลักษณะเฉพาะของการก่อการร้าย



***‘ผู้ก่อการร้ายของคนหนึ่งคือนักสู้เพื่ออิสรภาพของอีกคนหนึ่ง’*** (มุมมองทางการเมือง)

## การก่อการร้าย (Terrorism)

Pillar 1

**เป้าหมาย**
(Goal)

- อุดมการณ์ การเมือง ศาสนา สังคม (FBI)

Pillar 2

**ความรุนแรง**
(Violence)

- เจตนาทำให้เสียชีวิต บาดเจ็บ หรือจับตัวประกัน (UN Res 1566)

Pillar 3

**การข่มขู่**
(Coercion)

- ปลุกระดมให้เกิดความหวาดกลัว ขู่เข็ญบังคับรัฐบาล (กม.ไทย)

**การก่อการร้ายใช้ ‘ความกลัว’ เป็นอาวุธเพื่อบรรลุเป้าหมายทางการเมือง**

# พัฒนาการทางประวัติศาสตร์ของการก่อการร้าย

Academic Blueprint of Security

**ยุคโบราณ**

กลุ่ม Zealots และ Sicarii
ลอบสังหารต่อต้านอาณาจักรโรมัน
(Poland, 2011)

**1793–1794**

**‘ยุคสมัยแห่งความน่าสะพรึงกลัว’**
(Reign of Terror)
ฝรั่งเศส, รัฐบาลฌากอแบ็งกำจัด
ศัตรูทางการเมือง

**1914**

ลอบสังหาร Archduke
Franz Ferdinand
นำไปสู่สงครามโลกครั้งที่ 1

**1930s**

**‘การกวาดล้างใหญ่’**
(Great Purge)
ของสตาลินในโซเวียต
(ก่อการร้ายโดยรัฐ)

**การก่อการร้ายเป็นยุทธวิธีที่มีรากฐานฝังลึกในประวัติศาสตร์การเมืองโลก**

# การจำแนกประเภทของการก่อการร้าย



ไม่จำกัดแค่ซ้าย/ขวา แต่รวมถึงประเด็นเดียว หรือศาสนา/ชาติพันธุ์ (Dyson, 2011)

## Q1. แบบศาลเตี้ย (Vigilante)

ทำร้ายบุคคลโดยพลการเพื่อลงโทษ (เช่น KKK)

## Q2. ผู้ก่อความไม่สงบ (Insurgent)

แสวงหาการเปลี่ยนแปลงทางการเมืองในประเทศต่อต้านรัฐบาล

## Q3. ข้ามชาติ (Transnational)

วางแผนประเทศหนึ่ง โจมตีและปฏิบัติการในอีกประเทศหนึ่ง (เช่น 9/11)

## Q4. โดยรัฐ (State Terrorism)

รัฐบาลใช้ความรุนแรงกดขี่ประชาชนตนเอง

**การทำความเข้าใจประเภทกลุ่มก่อการร้าย ช่วยให้คาดการณ์เป้าหมายและยุทธวิธีได้**

# สาเหตุและรากฐานของการก่อการร้าย

Academic Blueprint of Security

**ความอยุติธรรม (Injustice):** การกดขี่ ความเหลื่อมล้ำทางเศรษฐกิจ การเหยียดเชื้อชาติ

**ภัยคุกคามทางวัฒนธรรม (Cultural Threat):** ความรู้สึกว่าศาสนาหรืออัตลักษณ์กำลังถูกทำลาย

**สาเหตุ (Causes)**

**ทฤษฎีการลิดรอนเชิงเปรียบเทียบ (Relative Deprivation Theory):** ความคับข้องใจเมื่อเปรียบเทียบสถานะที่เสียเปรียบของกลุ่มตนกับกลุ่มอื่นที่ได้ประโยชน์

**ข้อสังเกตทางสังคมวิทยา:** ผู้ก่อการร้ายมักมีเหตุผลทางการเมืองและสังคมมากกว่าปัญหาความเจ็บป่วยทางจิต

**การก่อการร้ายมักเกิดจากการตอบสนองต่อโครงสร้างทางสังคมที่เปราะบางและเหลื่อมล้ำ**

# ยุทธวิธีและอาวุธของผู้ก่อการร้าย



**ยุทธวิธี:** ระเบิดพลีชีพ, ลักพาตัว, จี้เครื่องบิน, โฆษณาชวนเชื่อ (Propaganda)

**เป้าหมาย:** เน้น เป้าหมายอ่อน (Soft Targets) เช่น ห้าง โรงเรียน มากกว่าเป้าหมายแข็งที่มีการป้องกัน

**IED (ระเบิดแสวงเครื่อง):** ประกอบง่ายจากของใช้ในบ้าน เป็นที่นิยมสูง

## WMD (อาวุธทำลายล้างสูง)

**C - Chemical** (เคมี)

**B - Biological** (ชีวภาพ)

**R - Radiological** (รังสี)

**N - Nuclear** (นิวเคลียร์)

**การจู่โจมเป้าหมายอ่อนโดยไม่มีการเตือนล่วงหน้า คือข้อได้เปรียบหลักของผู้ก่อการร้าย**

# บทสรุปวิชาการ คำถามท้ายบท และกิจกรรม



## บทสรุปวิชาการ

- องค์กรต้องเผชิญภัยคุกคามหลากหลาย (ไซเบอร์, อาชญากรรม, ภัยธรรมชาติ)
- ผู้ปฏิบัติงานต้องตรวจสอบจุดอ่อน วางกลยุทธ์ป้องกันเชิงรุก
- การเตรียมแผนความต่อเนื่อง (Business Continuity) คือกุญแจสำคัญ

## คำถามอภิปราย

1. ภัยคุกคาม (Threats) และอันตราย (Hazards) แตกต่างกันอย่างไร?
2. หากเกิดเหตุกราดยิงในมหาวิทยาลัย นักศึกษาควรปฏิบัติตัวอย่างไร?
3. การก่อการร้ายส่งผลต่อการจัดการห่วงโซ่อุปทานอย่างไร?

## กิจกรรมประยุกต์ (Risk Assessment)

จำลองสถานการณ์วิเคราะห์ช่องโหว่ (Soft Targets) ของโครงสร้างพื้นฐานวิทยาลัยและเสนอแนวทางป้องกัน

**ความมั่นคงไม่ใช่เรื่องบังเอิญ แต่เกิดจากการประเมินและวางแผนอย่างเป็นระบบ**