# ความเหมือน&ความแตกต่างระหว่าง

# IT SECURITY

# และ

# CYBER SECURITY


# ความเหมือน&ความแตกต่าง ระหว่าง IT SECURITY และ CYBER SECURITY

ปัจจุบันนี้ก้าวเข้าสู่โลกแห่งยุค IT อย่างเต็มรูปแบบ ซึ่ง IT หรือเทคโนโลยีสารสนเทศได้เปลี่ยนแปลงวิถีการดำเนินชีวิต การสื่อสาร รวมถึงการเรียน การสอน ที่มีการนำเทคโนโลยีมาใช้เพื่ออำนวยความสะดวก ทำให้เกิดการเปลี่ยนแปลงในด้านต่างๆ อย่างมากมาย อีกทั้งยังช่วยกระจายข้อมูลข่าวสารเป็นไปอย่างรวดเร็ว

แต่ในขณะเดียวกัน IT ก็อาจก่อให้เกิดโทษมหันต์ได้เช่นกัน หากนำไปใช้ในทางที่ผิด ซึ่งสิ่งเหล่านี้หากถูกนำไปใช้ในทางที่ถูกก็จะส่งผลดีให้แก่ตัวเรานั่นเอง

มหาวิทยาลัยมหิดล ได้ให้ความสำคัญด้านความปลอดภัย (Security) เพื่อช่วยในการป้องกันข้อมูลที่เป็นความลับและมีมูลค่าจากการถูกโจรกรรมมหาวิทยาลัยจึงต้องการระบบ Security ที่มีความปลอดภัยและเข้มแข็ง ควรจะมี IT Security และ Cyber Security

ในบทความนี้เรามาพิจารณาถึงความคล้ายคลึงกัน ความเหมือน ความแตกต่าง ระหว่าง IT Security และ Cyber security

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

**ความปลอดภัยทางข้อมูล**
***(INFORMATION SECURITY)***

คือ การรักษาข้อมูลที่อยู่ในรูปแบบ DIGITAL FORMAT หรือที่เรียกว่า DIGITAL INFORMATION ให้เป็นความลับ รวมไปถึงการจัดการข้อมูลให้พร้อมใช้งาน ซึ่งเป็นระบบรักษาความปลอดภัย ให้กับระบบสารสนเทศ

## CYBER SECURITY

**ความปลอดภัยทางไซเบอร์**
***(CYBER SECURITY)***

คือ วิธีลดความเสี่ยงจากการโจมตีทางอินเทอร์เน็ต ที่อาจส่งผลต่อการทำงาน อุปกรณ์ และบริการที่ใช้งาน ซึ่ง CYBER SECURITY ถือว่าเป็นตัวช่วยที่มีความสำคัญเป็นอย่างมาก เพราะสร้างความมั่นคงเกี่ยวกับความปลอดภัยของข้อมูลบนไซเบอร์

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

**IT SECURITY แบ่งเป็น 5 ประเภท**

1. ENDPOINT SECURITY

เป็นการรักษาความปลอดภัยให้แก่อุปกรณ์ปลายทาง เช่น โทรศัพท์มือถือ TABLETS LAPTOPS หรือ คอมพิวเตอร์ โดยเป็นการป้องกันเพื่อไม่ให้อุปกรณ์ที่ถูกใช้เหล่านี้เข้าถึงหน้าเว็บหรือเครือข่ายที่เป็นอันตรายซึ่งอาจจะก่อความเสียหายให้แก่องค์กรได้

## CYBER SECURITY

**CYBER SECURITY แบ่งเป็น 5 ประเภท**

1. CRITICAL INFRASTRUCTURE SECURITY

เป็นการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน เช่น ระบบนักศึกษา ระบบการเงิน ระบบในโรงพยาบาล ระบบต่าง ๆ ในมหาวิทยาลัย เป็นต้น ระบบโครงสร้างพื้นฐานเหล่านี้มักจะเชื่อมต่อกับอินเทอร์เน็ต ซึ่งง่ายต่อการถูกโจมตี ดังนั้นองค์กรควรให้ความสำคัญ และจัดทำแผนสำรองเมื่อเกิดเหตุฉุกเฉิน และแผนกู้คืนระบบ เพราะหากไม่มีแผนสำรอง จะทำให้เกิดความเสียหายอาจรุนแรงมากกว่าที่ควรจะเป็นได้

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

### 2. NETWORK SECURITY

เป็นการรักษาความปลอดภัยเครือข่าย มีไว้เพื่อป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตหรือเป็นอันตรายเข้ามาในเครือข่ายได้ นอกจากนี้ยังสามารถป้องกันไม่ให้แฮ็กเกอร์สามารถเข้าถึงข้อมูลในเครือข่ายอีกด้วย ซึ่งเป็นผลดีกับเจ้าของเครือข่ายมากทีเดียว แต่ปัจจุบัน NETWORK SECURITY เป็นเรื่องที่ค่อนข้างน่าหนักใจสำหรับองค์กรต่างๆเนื่องจากแต่ละองค์กรมีจำนวน ENDPOINT ค่อนข้างมากและยังย้ายไปสำรองข้อมูลใน PUBLIC CLOUD อีก ซึ่งยากต่อการควบคุม

## CYBER SECURITY

### 2. NETWORK SECURITY

เป็นการรักษาความปลอดภัยของระบบอินเทอร์เน็ต เพื่อป้องกันการถูกคุกคามจึงจำเป็นที่จะต้องมีระบบที่พัฒนามาเพื่อจัดการกับบุคคลภายนอกที่เข้ามาใช้งานโดยไม่ได้รับอนุญาตซึ่งอาจทำโดยการใช้MACHINE LEARNING บางตัวเพื่อรับส่งข้อมูลและคอยแจ้งเตือนถึงความผิดปกติก็ได้

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

### 3. INTERNET SECURITY

เป็นการรักษาความปลอดภัยอินเทอร์เน็ตในด้านการป้องกันข้อมูลที่ต้องรับและส่งใน BROWSER ตลอดจนการใช้งานผ่านทาง WEB APPLICATION ซึ่งถูกออกแบบมาเพื่อตรวจสอบข้อมูลที่รับส่งเข้ามาทางอินเทอร์เน็ตและตรวจสอบมัลแวร์ หลาย ๆ องค์กรใช้ FIREWALL โปรแกรม ANTIMALWARE และ โปรแกรม ANTISPYWARE ในการป้องกัน

## CYBER SECURITY

### 3. INTERNET OF THING SECURITY

อุปกรณ์ในปัจจุบันที่สามารถเชื่อมต่อกับอินเตอร์เน็ตเพื่อผู้ใช้สั่งงานหรือตั้งค่าอุปกรณ์ได้หรือที่เรียกกันสั้น ๆ ว่า IOT ก็ต้องได้รับการรักษาความปลอดภัย เนื่องจากการส่งข้อมูลถึงอุปกรณ์ IOT ต้องทำผ่านอินเตอร์เน็ต และ อุปกรณ์ IOT อาจสามารถส่งข้อมูลถึงกันผ่านอินเตอร์เน็ตได้ ดังนั้นจึงต้องมี IOT SECURITY เพื่อใช้เป็นมาตรการในการรักษาความปลอดภัยให้องค์กรต่าง ๆ

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

### 4. APPLICATION SECURITY

เป็นการรักษาความปลอดภัยในการเข้าใช้แอปพลิเคชันต่าง ๆ โดยผู้ใช้จะได้รับรหัสเฉพาะ เพื่อยืนยันตัวตน หรือเป็นการยืนยันว่าระบบจะไม่ถูกโจมตี
ซึ่งข้อดีของการมี APPLICATION SECURITY ก็คือ ทางองค์กรสามารถประเมินได้ว่าระบบมีช่องโหว่ในซอฟต์แวร์ตรงไหนบ้าง


## CYBER SECURITY

### 4. APPLICATION SECURITY

เป็นการรักษาความปลอดภัยในระบบ APPLICATION เช่น โปรแกรม ANTIVIRUS FIREWALL หรือโปรแกรมการเข้ารหัส ซึ่งจะมีการใช้ทั้ง HARDWARE และ SOFTWARE ควบคู่กันไปเพื่อจัดการกับภัยคุกคามที่เกิดขึ้น ในปัจจุบันภัยคุกคามมักจะเกิดขึ้นตอน APPLICATION อยู่ในขั้นตอนที่กำลังพัฒนา ดังนั้นการมี APPLICATION SECURITY จึงเป็นอีกทางเลือกหนึ่งในการป้องกันข้อมูลใน APPLICATION

# IT SECURITY VS CYBER SECURITY

## IT SECURITY

### 5. CLOUD SECURITY

ถือเป็นระบบที่สามารถช่วยรักษาความปลอดภัยให้กับแอปพลิเคชั่นต่างๆ มีตัวกลางที่คอยจัดการเข้าถึง ตลอดจนการจัดการภัยคุกคามบนคลาวด์ได้อีกด้วย

## CYBER SECURITY

### 5. CLOUD SECURITY

เป็นการรักษาความปลอดภัยให้กับข้อมูลที่เก็บลงในคลาวด์ โดยไม่ต้องเสียค่าใช้จ่ายและเวลาในการดูแล SERVER

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## IT SECURITY

RANSOMWARE

**RANSOMWARE (ไวรัสเรียกค่าไถ่)**

ไวรัสคอมพิวเตอร์ประเภทนี้ สามารถป้องกันได้โดยการติดตั้งโปรแกรม ANTI-VIRUS ที่ได้รับการอัปเดต และทำการสแกนอยู่เสมอ หรือทำการสำรองข้อมูลที่สำคัญเอาไว้หลายๆแห่ง

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## IT SECURITY

SPYWARE

### SPYWARE

การขโมยข้อมูลจากไดร์ฟผู้ใช้งาน ทั้งข้อมูลส่วนตัว และไฟล์งาน สามารถป้องกันได้โดย การตั้งค่าความเป็นส่วนตัวในคอมพิวเตอร์ ไม่เปิดอีเมลจากผู้ที่ไม่รู้จัก และดาวน์โหลดไฟล์จากเว็บที่ได้รับการยืนยันแล้วเท่านั้น

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## IT SECURITY

VIRUSES

### VIRUSES

มัลแวร์ที่สามารถทำลายโปรแกรมหรือข้อมูลในคอมพิวเตอร์ป้องกันได้โดยการไม่เชื่อมต่ออุปกรณ์แปลกๆ ที่ไม่ได้รับการสแกนไวรัสเข้ากับเครื่อง

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## CYBER SECURITY

CYBERCRIME

**CYBERCRIME (อาชญากรรมไซเบอร์)**

การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อื่นๆเพื่อทำลายระบบหรือขโมยข้อมูลสำคัญต่างๆ

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## CYBER SECURITY


CYBER-ATTACK

### CYBER-ATTACK

เป็นการโจมตีเพื่อขโมยข้อมูลชนิดหนึ่ง สามารถพบได้บ่อยๆ เช่น ก่อกวนเครือข่าย ปลอมหน้าเว็บไซต์ ติดตั้งโปรแกรมประสงค์ร้าย

# ภัยคุกคามจากเทคโนโลยีสารสนเทศ (THREATS OF INFORMATION TECHNOLOGY)

## CYBER SECURITY

CYBERTERRORISM

**CYBERTERRORISM**

การก่อการร้ายทางไซเบอร์ เช่น ระบบคอมพิวเตอร์หรือเครือข่ายโทรคมนาคม ซึ่งการติดตามตัวผู้กระทำความผิดทำได้ยากหากเกิดเหตุอาจสูญเสียข้อมูลที่เป็นความลับสำคัญ

# ความคล้ายคลึงระหว่าง IT SECURITY และ CYBER SECURITY

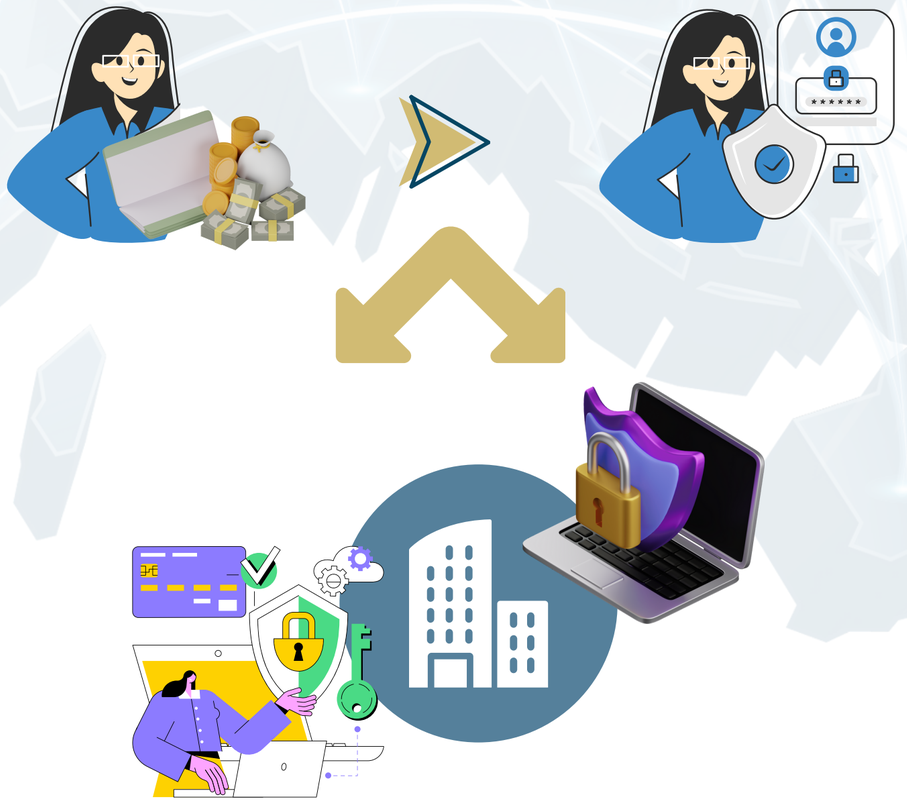
## IT SECURITY และ CYBERSECURITY

ค่อนข้างมีความคล้ายคลึงกันซึ่งอาจจะทำให้เกิดความสับสนได้ ทั้งสองสิ่ง หมายถึง แนวทางปฏิบัติที่มีจุดมุ่งหมายเพื่อรักษาความปลอดภัยและป้องกันระบบคอมพิวเตอร์จากการถูกละเมิดข้อมูล

นอกจากนี้ ทั้ง IT SECURITY และ CYBERSECURITY ยังมีกระบวนการทำงานที่คล้าย ๆ กันและส่งเสริมกันอีกด้วย แต่ละองค์กรจะต้องมี IT SECURITY เพื่อรักษาความปลอดภัยให้กับข้อมูลในคอมพิวเตอร์ และจะต้องมี CYBERSECURITY เพื่อรักษาความปลอดภัยให้กับข้อมูลอิเล็กทรอนิกส์ (ข้อมูลที่ออนไลน์อยู่บนโลกไซเบอร์)

ทั้งสองสิ่งนี้เป็นเหมือนกุญแจสำคัญในการรักษาข้อมูลต่าง ๆ ยิ่งไปกว่านั้น ทั้งสองสิ่งยังต้องทำหน้าที่รับประกันมูลค่าของข้อมูลอีกด้วย

**ตัวอย่างเช่น:** ผู้ใช้งานมีบัญชีธนาคาร องค์กรจะต้องมี IT SECURITY และ CYBERSECURITY เพื่อป้องกันไม่ให้รหัส PIN ของผู้ใช้งานรั่วไหล และจะต้องเก็บข้อมูลส่วนตัวของผู้ใช้งานไว้เป็นความลับให้ได้ เป็นต้น



# มาตรฐานการรักษาความปลอดภัยของข้อมูล

การสร้างมาตรฐานการรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพและเหมาะสมเป็นสิ่งสำคัญ อย่างยิ่งในปัจจุบันองค์กรจำเป็นจะต้องคำนึงถึง CIA เสมอ


**CONFIDENTIALITY**
(การรักษาความลับของข้อมูล)

คือ การระบุสิทธิในการเข้าถึงข้อมูลให้กับผู้ที่ได้ใบอนุญาติให้สามารถเข้าถึงแต่ละชุดข้อมูลตามลำดับชั้นความลับที่กำหนดไว้เท่านั้น

**INTEGRITY**
(การรักษาความถูกต้องของข้อมูล)

คือ การระบุสิทธิในการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง


**AVAILABILITY**
(ความพร้อมใช้งานของข้อมูล)

คือ การทำให้ข้อมูลพร้อมให้เข้าถึงและใช้งานได้ตลอดเวลา มีการรักษาความต่อเนื่องในการให้บริการข้อมูล

**แหล่งที่มา:**
https://pdpa.pro/blogs/how-cyber-security-and-it-security-are-important-for-data-protection
https://techspace.co.th/blog/it-network-cyber-security/

**ผู้รวบรวมข้อมูล:** นางสาวนันทนิตร์ มีพร้อม
ศูนย์ตรวจภายใน
มหาวิทยาลัยมหิดล