แบบทดสอบ

เริ่มเมื่อ	พฤหัสบดี, 10 ตุลาคม 2024, 4:36PM
State	เสร็จสิ้น
เมื่อ	พฤหัสบดี, 10 ตุลาคม 2024, 5:28PM
เวลาที่ใช้	51 นาที 53 วินาที
คะแนน	19.00/30.00
คะแนน	จากคะแนนเต็ม

คำถาม 1

เสร็จสิ้น

Mark 1.00 out of 1.00

วัตถุประสงค์ของการดำเนินการควบคุมความปลอดภัยในกระบวนการบริหารความเสี่ยงคืออะไร? (What is the purpose of implementing security controls in the risk management process?)

a. **เพื่อขจัดช่องโหว่ทั้งหมด** (To eliminate all vulnerabilities)

b. **เพื่อเพิ่มระดับความเสี่ยง** (To increase the level of risk)

c. **เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้** (To mitigate the risk to an acceptable level)

d. **เพื่อให้แน่ใจว่าการโจมตีทางไซเบอร์จะเป็นไปไม่ได้** (To ensure that a cyberattack would be impossible)

คำถาม 2

เสร็จสิ้น

Mark 1.00 out of 1.00

ช่องโหว่ในบริบทของความมั่นคงปลอดภัยคืออะไร? (What is a vulnerability in the context of security?)

- a. จุดอ่อนหรือข้อบกพร่องที่มีอยู่ในระบบหรือส่วนประกอบ (An inherent weakness or flaw in a system or component)
- b. ขั้นตอนที่ดำเนินการเพื่อกีดกันผู้กระทำภัยคุกคาม (The steps taken to discourage threat actors)
- c. การกระทำที่ถูกมุ่งเป้าโดยผู้กระทำภัยคุกคาม (The act of being targeted by threat actors)
- d. กระบวนการลดความน่าสนใจขององค์กรในฐานะเป้าหมาย (The process of decreasing the organization's attractiveness as a target)

คำถาม 3

เสร็จสิ้น

Mark 1.00 out of 1.00

คำว่าใดที่ใช้เพื่ออธิบายการให้สิทธิ์การเข้าถึงแก่ผู้ใช้หลังจากแสดงวิธีการพิสูจน์ตัวตนสองวิธีหรือมากกว่านั้นสำเร็จ? (What is the term used to describe granting users access only after successfully demonstrating two or more methods of authentication?)

- a. การพิสูจน์ตัวตนแบบปัจจัยเดียว (SFA) (Single-factor authentication) (SFA)
- b. การพิสูจน์ตัวตนแบบหลายปัจจัย (MFA) (Multi-factor authentication) (MFA)
- c. การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะ (Characteristic-based authentication)
- d. การพิสูจน์ตัวตนโดยใช้โทเค็น (Token-based authentication)

คำถาม 4

เสร็จสิ้น

Mark 0.00 out of 1.00

อะไรคือความท้าทายหลักในการรักษาความลับของข้อมูล เมื่อต้องจัดการกับผู้ใช้ระบบที่อาจกำลังเข้าถึงระบบจากเครื่องคอมพิวเตอร์ที่ถูกบุกรุก หรือแอปพลิเคชันมือถือที่มีช่องโหว่? (What is the main challenge in achieving confidentiality when dealing with system users who may be accessing the system from compromised machines or vulnerable mobile applications?)

- a. การระบุข้อมูลที่ละเอียดอ่อน (Identifying sensitive information)
- b. การป้องกันจากผู้มีส่วนได้เสียภายนอก (Defending against external stakeholders)
- c. การสร้างสมดุลระหว่างการเข้าถึงที่ได้รับอนุญาตและการปกป้องข้อมูล (Balancing authorized access and data protection)
- d. การควบคุมการเข้าถึงเพื่อปกป้องข้อมูล (Regulating access to protect data)

คำถาม 5

เสร็จสิ้น

Mark 1.00 out of 1.00

สถานการณ์: ทีมรักษาความปลอดภัยขององค์กรวิเคราะห์องค์กรของตนจากมุมมองของผู้กระทำภัยคุกคามเพื่อทำความเข้าใจว่าทำไมพวกเขาถึงอาจเป็นเป้าหมายที่น่าสนใจ เป้าหมายของการวิเคราะห์นี้คืออะไร?(Scenario: An organization's security team analyzes their organization from the perspective of a threat actor to understand why they might be an attractive target. What is the goal of this analysis?)

- a. การเรียนรู้เกี่ยวกับภัยคุกคาม (Learning about threats)
- b. การลดช่องโหว่ (Decreasing vulnerability)
- c. การระบุช่องโหว่ (Identifying vulnerabilities)
- d. การกีดกันผู้กระทำภัยคุกคาม (Discouraging threat actors)

คำถาม 6

เสร็จสิ้น

Mark 1.00 out of 1.00

ปรีชากำลังพิจารณาซื้อสินค้าออนไลน์ ผู้ขายขอให้เขาสร้างบัญชีผู้ใช้ใหม่โดยต้องกรอกข้อมูลส่วนตัว เช่น ชื่อเต็ม ที่อยู่ หมายเลขบัตรเครดิต เบอร์โทรศัพท์ และอีเมล นอกจากนี้ยังขออนุญาตใช้ข้อมูลเพื่อส่งข้อความทางการตลาดและแบ่งปันกับผู้ขายรายอื่น ปรีชาประเมินแล้วว่าสินค้าไม่คุ้มค่ากับการเปิดเผยข้อมูลส่วนตัว จึงตัดสินใจไม่ซื้อ การกระทำของปรีชาในกรณีนี้ถือเป็นการบริหารความเสี่ยงแบบใด? (Precha is deciding whether to make an online purchase. The vendor wants Precha to create a new user account and requests Precha's full name, home address, credit card number, phone number, email address, the ability to send marketing messages to Precha, and permission to share this data with other vendors. Precha decides that the item for sale is not worth the value of Precha's personal information, and she decides not to make the purchase. What kind of risk management approach did Precha take?)

a. การยอมรับความเสี่ยง (Acceptance)

b. การบรรเทาหรือลดทอนความเสี่ยง (Mitigation)

c. การถ่ายโอนความเสี่ยง (Transfer)

d. การหลีกเลี่ยงความเสี่ยง (Avoidance)

คำถาม 7

เสร็จสิ้น

Mark 1.00 out of 1.00

วัตถุประสงค์ของนโยบายการเก็บรักษาในแนวปฏิบัติการจัดการข้อมูลคืออะไร? (What is the purpose of retention policies in data handling practices?)

- a. **เพื่อให้แน่ใจว่าปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับ** (To ensure compliance with legal and regulatory requirements)
- b. **เพื่อกำหนดระดับความอ่อนไหวของข้อมูล** (To define the sensitivity levels of data)
- c. **เพื่อใช้งานการเข้ารหัสเพื่อการป้องกันข้อมูล** (To implement encryption for data protection)
- d. **เพื่อกำหนดฉลากให้กับข้อมูลตามมูลค่าของมัน** (To assign labels to data based on its value)

คำถาม 8

เสร็จสิ้น

Mark 1.00 out of 1.00

วิธีที่แนะนำในการลดการคงค้างของข้อมูลคืออะไร? (What is the recommended method for reducing data remanence?)

- a. **ล้างอุปกรณ์โดยการเขียนทับด้วยค่าที่สุ่ม** (Clearing the device by overwriting with random values)
- b. **ทำการสำรองข้อมูลเป็นประจำ** (Performing regular data backups)
- c. **เก็บข้อมูลในสถานที่ที่ปลอดภัยนอกสถานที่** (Storing the data in a secure off-site location)
- d. **เข้ารหัสข้อมูลก่อนการลบ** (Encrypting the data before deletion)

คำถาม 9

เสร็จสิ้น

Mark 1.00 out of 1.00

ไฟล์บันทึกขององค์กรถูกแก้ไขหรือลบ ทำให้ความสมบูรณ์ของข้อมูลบันทึกถูกละเมิด ดังนั้นควรดำเนินการมาตรการใดเพื่อแก้ไขปัญหานี้? (An organization's log files have been edited or deleted, compromising the integrity of the log datA) Which measure should be taken to address this issue?)

a. เพิ่มความจุในการจัดเก็บของสื่อไฟล์บันทึก (Increase the storage capacity of log file media)

b. ทำการตรวจสอบบันทึกเป็นประจำ (Perform regular log reviews)

c. ใช้มาตรการควบคุมเพื่อป้องกันการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต (Implement controls to protect against unauthorized changes)

d. ตรวจสอบการจราจรขาเข้าและขาออก (Monitor ingress and egress traffic)

คำถาม 10

เสร็จสิ้น

Mark 0.00 out of 1.00

อะไรควรเป็นจุดเน้นหลักของการฝึกอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยของข้อมูล? (What should be the primary focus of awareness training for information security?)

a. การสร้างสภาพแวดล้อมที่เน้นการลงโทษ (Creating a punitive environment)

b. การระบุและลงโทษบุคคลที่ละเมิดความปลอดภัย (Identifying and penalizing individuals for security breaches)

c. การส่งเสริมประสบการณ์เชิงบวกสำหรับทุกคน (Promoting a positive experience for everyone)

d. การรับรองการปฏิบัติตามนโยบายและขั้นตอนอย่างเคร่งครัด (Ensuring strict adherence to policies and procedures)

คำถาม 11

เสร็จสิ้น

Mark 1.00 out of 1.00

ทำไมวิธีการโจมตีแบบ social engineering จึงมีประสิทธิภาพ? (Why does social engineering work effectively as an attack method?)

a. เพราะมันอาศัยซอฟต์แวร์ที่ซับซ้อน (It relies on sophisticated software)

b. เพราะมันใช้ประโยชน์จากแนวโน้มพฤติกรรมของมนุษย์ (It exploits human tendencies)

c. เพราะมันเกี่ยวข้องกับทักษะทางเทคนิคขั้นสูง (It involves advanced technical skills)

d. เพราะมันต้องการการเข้าถึงระบบทางกายภาพ (It requires physical access to systems)

คำถาม 12

เสร็จสิ้น

Mark 1.00 out of 1.00

วัตถุประสงค์ของนโยบายการเก็บรักษาในแนวปฏิบัติการจัดการข้อมูลคืออะไร? (What is the purpose of data retention policies in data handling practices?)

a. เพื่อใช้งานการเข้ารหัสเพื่อการป้องกันข้อมูล (To implement encryption for data protection)

b. เพื่อให้แน่ใจว่าข้อมูลถูกเก็บไว้ในระยะเวลาที่จำเป็นหรือมีประโยชน์ (To ensure data is kept for the required or useful period)

c. เพื่อกำหนดข้อกำหนดการติดฉลากสำหรับข้อมูล (To define the labeling requirements for data)

d. เพื่อกำหนดความอ่อนไหวของข้อมูล (To determine the sensitivity of data)

คำถาม 13

เสร็จสิ้น

Mark 1.00 out of 1.00

สถานการณ์ใดต่อไปนี้แสดงให้เห็นถึงหลักการของสิทธิพิเศษน้อยที่สุดได้ดีที่สุด? (Which of the following scenarios best exemplifies the Principle of Least Privilege?)

a. เฉพาะบุคคลที่ได้รับอนุญาตในแผนกการเรียกเก็บเงินเท่านั้นที่สามารถดูและแก้ไขข้อมูลทางการเงินของผู้บริโภคได้ (Only authorized individuals in the billing department can view and modify consumer financial data.)

b. พนักงานทุกคนสามารถเข้าถึงข้อมูลลูกค้าที่เป็นความลับได้โดยไม่จำกัด (All employees have unrestricted access to confidential customer data.)

c. ผู้ใช้ทุกคนในองค์กรมีสิทธิ์เข้าถึงระบบและแอปพลิเคชันทั้งหมดในระดับผู้ดูแลระบบ (Every user in the organization has administrative access to all systems and applications.)

d. พนักงานสามารถเข้าถึงไฟล์และโฟลเดอร์ทั้งหมดบนเครือข่ายได้โดยไม่มีข้อจำกัด (Employees can access all files and folders on the network without restrictions.)

คำถาม 14

เสร็จสิ้น

Mark 0.00 out of 1.00

ในระบบการควบคุมการเข้าถึงแบบบังคับ (MAC) ใครมีอำนาจในการแก้ไขกฎความปลอดภัยสำหรับผู้ใช้และทรัพยากร? (In a Mandatory Access Control (MAC) system, who has the authority to modify security rules for subjects and objects?)

a. ผู้ใช้งานแต่ละคน (Individual users)

b. ผู้ดูแลระบบ (System administrators)

c. เจ้าของสินทรัพย์ (Asset owners)

d. ผู้ดูแลระบบด้านความปลอดภัย (Security administrators)

คำถาม 15

เสร็จสิ้น

Mark 0.00 out of 1.00

สิทธิ์ของพนักงานระดับล่างถูกขยายชั่วคราวให้ทำหน้าที่เป็นผู้จัดการแผนก ปัญหาที่อาจเกิดขึ้นหากไม่มีการเปลี่ยนสิทธิ์กลับคืนคืออะไร? (A junior worker's permissions are temporarily expanded to act as a department manager. What potential issue can occur if their permissions are not changed back?)

a. บทบาทไม่ตรงกัน (Role mismatch)

b. การคืบคลานของสิทธิพิเศษ (Privilege creep)

c. การกำหนดค่าการควบคุมการเข้าถึงผิดพลาด (Access control misconfiguration)

d. สิทธิ์การเข้าถึงไม่เพียงพอ (Insufficient access privileges)

คำถาม 16

เสร็จสิ้น

Mark 0.00 out of 1.00

ตัวอย่างใดแสดงถึงการควบคุมความปลอดภัย? (Which example represents a security control?)

a. การกำหนดสามเหลี่ยม CIA (Defining the CIA Triad)

b. การเข้ารหัสข้อมูลที่ละเอียดอ่อน (Encrypting sensitive data)

c. การจำกัดการเข้าถึงวัตถุ ผู้ใช้ และกฎ (Limiting access to objects, subjects, and rules)

d. การติดตั้งไฟร์วอลล์เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต (Installing a firewall to prevent unauthorized access)

คำถาม 17

เสร็จสิ้น

Mark 0.00 out of 1.00

มาตรการบางอย่างที่ใช้เพื่อลดความเสี่ยงที่เกี่ยวข้องกับบัญชีที่มีสิทธิพิเศษคืออะไร? (What are some measures used to mitigate risks associated with privileged accounts?)

a. การตรวจสอบสิทธิ์ที่เข้มงวดขึ้นสำหรับผู้ใช้ที่ไม่มีสิทธิพิเศษ (Stricter authentication for non-privileged users.)

b. การตรวจสอบบัญชีผู้ใช้ทั่วไปอย่างละเอียดมากขึ้น (Auditing regular user accounts more extensively.)

c. การตรวจสอบประวัติและการตรวจสอบทางการเงินเป็นประจำ (Regular background checks and financial investigation.)

d. การบันทึกและการควบคุมการเข้าถึงที่จำกัด (Limited logging and access control.)

คำถาม 18

เสร็จสิ้น

Mark 1.00 out of 1.00

ในสภาพแวดล้อม UNIX ที่มีการควบคุมการเข้าถึงแบบเลือกได้ (DAC) ปรีชาได้สร้างไฟล์และให้สิทธิ์ มนตรีในการเข้าถึงและแก้ไขไฟล์นั้น สถานการณ์นี้แสดงให้เห็นถึงอะไร? (In a UNIX environment with discretionary access control (DAC) in place, Precha has created a file and granted Montri permission to access and modify it. What does this scenario demonstrate?)

a. การควบคุมการเข้าถึงตามบทบาท (RBAC) (Role-based access control) (RBAC)

b. การควบคุมการเข้าถึงตามกฎ (Rule-based access control)

c. การควบคุมการเข้าถึงตามดุลยพินิจ (DAC) (Discretionary access control) (DAC)

d. หลักการของสิทธิ์ที่น้อยที่สุด (The principle of least privilege)

คำถาม 19

เสร็จสิ้น

Mark 0.00 out of 1.00

รูปแบบบริการคลาวด์แบบใดที่ให้การเข้าถึงแอปพลิเคชันซอฟต์แวร์ที่โฮสต์โดยผู้ขายหรือผู้ให้บริการคลาวด์? (Which cloud service model provides access to software applications hosted by a vendor or cloud service provider?)

- a. บริการแบบติดตั้งในองค์กร (On-Premises Service - OPS)
- b. แพลตฟอร์มเป็นบริการ (Platform as a Service - PaaS)
- c. โครงสร้างพื้นฐานเป็นบริการ (Infrastructure as a Service - IaaS)
- d. ซอฟต์แวร์เป็นบริการ (Software as a Service - SaaS)

คำถาม 20

เสร็จสิ้น

Mark 1.00 out of 1.00

สถานการณ์: ผู้ใช้ได้รับอีเมลที่มีลิงก์หลอกลวงไปยังเว็บไซต์ที่เป็นอันตราย ภัยคุกคามทางไซเบอร์ประเภทนี้คืออะไร? (Scenario: A user receives an email that contains a fraudulent link to a malicious website. What type of cyber threat is this?)

- a. การโจมตีแบบปฏิเสธการให้บริการ (DoS attack)
- b. ไวรัสคอมพิวเตอร์ (Computer virus)
- c. การปลอมแปลง (Spoofing)
- d. การหลอกลวงทางอินเทอร์เน็ต (Phishing)

คำถาม 21

เสร็จสิ้น

Mark 0.00 out of 1.00

ชั้นใดของโมเดล OSI ที่รับผิดชอบในการเพิ่มที่อยู่ปลายทางให้กับเฟรมข้อมูลเพื่อสร้างแพ็กเก็ต? (Which layer of the OSI model is responsible for adding destination addresses to the data frames to create packets?)

- a. Application Layer
- b. Physical Layer
- c. Network Layer
- d. Data Link Layer

คำถาม 22

เสร็จสิ้น

Mark 1.00 out of 1.00

ชั้นใดของโมเดล OSI ที่รับผิดชอบในการส่งเฟรมในเครือข่าย? (Which layer of the OSI model is responsible for sending frames in a network?)

- a. Data Link Layer
- b. Physical Layer
- c. Application Layer
- d. Presentation Layer

คำถาม 23

เสร็จสิ้น

Mark 1.00 out of 1.00

เมื่อข้อมูลเคลื่อนขึ้นไปตามชั้นของโมเดล OSI จาก Physical Layer ไปยัง Application Layer กระบวนการใดเกิดขึ้น? (When data moves up the layers of the OSI model from Physical to Application, what process occurs?)

- a. การประกอบใหม่ (Reassembly)
- b. การห่อหุ้ม (Encapsulation)
- c. การแบ่งส่วน (Segmentation)
- d. การแกะห่อ (De-encapsulation)

คำถาม 24

เสร็จสิ้น

Mark 1.00 out of 1.00

วัตถุประสงค์ของ IP Address ในเครือข่ายคืออะไร? (What is the purpose of an IP address in networking?)

- a. กรองการจราจรของเครือข่าย (Filtering network traffic)
- b. กำหนด MAC Address ให้กับอุปกรณ์ (Assigning MAC addresses to devices)
- c. ให้ที่อยู่เชิงตรรกะ (logical addresses) สำหรับอินเทอร์เฟซเครือข่าย (Providing logical addresses for network interfaces)
- d. กำหนดการเชื่อมต่อแบบมีสายระหว่างอุปกรณ์เครือข่าย (Defining wired connections between networked devices)

คำถาม 25

เสร็จสิ้น

Mark 0.00 out of 1.00

อะไรคือผลลัพธ์สำคัญของการวิเคราะห์ผลกระทบทางธุรกิจ (BIA)? (What is a key outcome of a Business Impact Analysis (BIA)?)

- a. ความสำคัญของพนักงานบริการลูกค้า (Importance of customer service staff)
- b. การระบุหน้าที่และการพึ่งพาต่างๆ (Identification of functions and dependencies)
- c. ผลกระทบทันทีต่อพื้นที่การทำงานอื่นๆ (Immediate effect on other areas of work)
- d. การเปลี่ยนไปใช้พื้นที่สำนักงานถาวร (Transition to permanent office space)

คำถาม 26

เสร็จสิ้น

Mark 0.00 out of 1.00

ทำไมจึงจำเป็นต้องพิจารณาไม่เพียงแค่ระดับเซิร์ฟเวอร์ แต่รวมถึงฐานข้อมูลและการพึ่งพาระบบอื่นๆ ในแผนกู้คืนจากภัยพิบัติสำหรับระบบที่ซับซ้อน? (Why is it necessary to consider not only the server level but also the database and dependencies on other systems in disaster recovery plans for complex systems?)

a. เพื่อจัดการกับการพึ่งพากันอย่างซับซ้อนของระบบต่างๆ (To address the intricate dependencies of the systems)

b. เพื่อทำให้กระบวนการกู้คืนจากภัยพิบัติมีประสิทธิภาพมากขึ้น (To streamline the disaster recovery process)

c. เพื่อปฏิบัติตามข้อกำหนดทางกฎหมาย (To comply with legal regulations)

d. เพื่อลดค่าใช้จ่ายในการจัดเก็บข้อมูล (To reduce storage costs)

คำถาม 27

เสร็จสิ้น

Mark 0.00 out of 1.00

ในระหว่างการตอบสนองต่อเหตุการณ์ ทีมตอบสนองต่อเหตุการณ์จะวิเคราะห์ข้อมูลที่มีอยู่และข้อมูลข่าวกรองภัยคุกคามเพื่อทำความเข้าใจลักษณะของเหตุการณ์และจัดลำดับความสำคัญของการตอบสนอง กิจกรรมนี้อยู่ในส่วนประกอบใดของแผนการตอบสนองต่อเหตุการณ์? (During an incident response, the incident response team analyzes the available data and threat intelligence to understand the nature of the incident and prioritize the response. Which component of the incident response plan does this activity belong to?)

a. การเตรียมการ (Preparation)

b. การกักกัน (Containment)

c. การตรวจจับและการวิเคราะห์ (Detection and Analysis)

d. กิจกรรมหลังเหตุการณ์ (Post-Incident Activity)

คำถาม 28

เสร็จสิ้น

Mark 1.00 out of 1.00

ส่วนประกอบใดของแผนการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับการพัฒนานโยบายที่ได้รับการอนุมัติจากผู้บริหาร? (Which component of the incident response plan involves developing a policy approved by management?)

- a. กิจกรรมหลังเหตุการณ์ (Post-Incident Activity)
- b. การตรวจจับและการวิเคราะห์ (Detection and Analysis)
- c. การเตรียมการ (Preparation)
- d. การกักกัน (Containment)

คำถาม 29

เสร็จสิ้น

Mark 1.00 out of 1.00

ทำไมสมาชิกทีมกู้คืนภัยพิบัติที่สำคัญจึงต้องมีรายการตรวจสอบในสถานการณ์ภัยพิบัติ? (Why do critical disaster recovery team members require checklists in a disaster situation?)

- a. เพื่อแก้ไขปัญหาทางเทคนิคระหว่างการกู้คืน (To troubleshoot technical issues during recovery)
- b. เพื่อเป็นแนวทางในการปฏิบัติงานท่ามกลางบรรยากาศที่วุ่นวายของภัยพิบัติ (To guide their actions amid the chaotic atmosphere of a disaster)
- c. เพื่อให้แน่ใจว่ามีการสื่อสารกับสาธารณชนอย่างมีประสิทธิภาพ (To ensure effective communication with the public)
- d. เพื่อรักษาการดำเนินงานเฉพาะของแต่ละแผนก (To maintain department-specific operations)

คำถาม 30

เสร็จสิ้น

Mark 1.00 out of 1.00

คำจำกัดความของอุบัติการณ์คืออะไร? (What is the definition of an incident?)

a. เหตุการณ์ความปลอดภัยที่เกิดขึ้นโดยเจตนาที่เกี่ยวข้องกับผู้บุกรุก (Deliberate security incident involving an intruder)

b. การเกิดขึ้นที่สังเกตได้ในเครือข่ายหรือระบบ (Observable occurrence in a network or system)

c. การสูญเสียการควบคุมหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต (Loss of control or unauthorized disclosure of personally identifiable information)

d. เหตุการณ์ที่เป็นอันตรายต่อความลับ ความสมบูรณ์ หรือความพร้อมใช้งานของระบบข้อมูล (Event that jeopardizes the confidentiality, integrity, or availability of an information system)