Question 2  
ประโยชน์ของการทำ Performance Development Review (PDR) คืออะไร และเป็นอย่างไรที่จะช่วยให้พนักงานและองค์กรประสบความสำเร็จ?

Performance Development Review (PDR) เป็นกระบวนการประเมินผลและวางแผนพัฒนาทักษะของพนักงาน โดยมุ่งเน้นการตรวจสอบประสิทธิภาพการทำงาน ช่วยให้พนักงานเข้าใจเป้าหมายขององค์กรและหาวิธีการพัฒนา

Question 1  
องค์กรจะสามารถนำหลักการ CIA ไปใช้ในกลยุทธ์การรักษา ความปลอดภัยข้อมูลได้อย่างไร

เพื่อให้มั่นใจถึงประสิทธิภาพของการท าการรักษาความปลอดภัยและตรงตาม วัตถุประสงค์ของ CIA ทางองค์กรต้องท าการด าเนินการประเมินความปลอดภัยอยู่เป็น ประจ า ซึ่งรวมถึงการทดสอบการเจาะระบบอีกด้วย โดยการระบุช่องโหว่กับช่องว่างใน การควบคุมความปลอดภัยออกมาอย่างชัดเจน ท าให้องค์กรสามารถท าการปรับปรุงด้าน ความปลอดภัยได้อย่างเป็นขั้นเป็นตอน

Question 4  
ผลที่อาจเกิดขึ้นจากการโจมตีเครือข่ายที่ประสบความสำเร็จ คืออะไร และองค์กรจะบรรเทาผลกระทบเหล่านี้ได้อย่างไร

ผลที่ตามมาของการโจมตีเครือข่ายที่ประสบความสำเร็จ อาจรุนแรงและรวมถึงการสูญเสียทางการเงิน ความ เสียหายต่อชื่อเสียง และผลทางกฎหมายและข้อบังคับ ตัวอย่างเช่น การโจมตีที่ประสบความสำเร็จอาจส่งผลให้ เกิดการขโมยข้อมูลที่ละเอียดอ่อน สิ่งนี้อาจนำไปสู่การ สูญเสียทางการเงิน นอกจากนี้ การโจมตีที่ประสบ ความสำเร็จอาจทำลายชื่อเสียงขององค์กรและทำลายความ ไว้วางใจของลูกค้า ซึ่งอาจส่งผลกระทบระยะยาวต่อผลกำไร ขององค์กร เพื่อลดผลกระทบเหล่านี้ องค์กรควรมีแผน รับมือเหตุการณ์ที่มีประสิทธิภาพซึ่งรวมถึงขั้นตอนในการ ตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย ภายในองค์กร และส่งเสริมความตระหนักด้านความ ปลอดภัยและการศึกษาแก่พนักงานทุกระดับ

Question 3  
อะไรคือจุดประสงค์ในการท า network topology diagram

จุดประสงค์หลักของการท า network topology diagram เนื่องจากเป็นรูปที่ แสดงระบบ network ทั้งแบบ physical ที่จะเห็นแค่รูปภาพโครงสร้างและในแบบ logical ที่จะแสดงทั้งรูปแบบการต่อต่ออย่างไรและมีเลข IP อะไรอยู่ตรงไหนบ้าง อีก ทั้งการท า diagram ช่วยลดการผิดพลาดและช่วยท าให้การหาข้อผิดพลาดเมื่อเกิดขึ้น ท าได้ง่ายขึ้น

Question 5  
อะไรคือความแตกต่างระหว่าง stateful and stateless firewalls?

Stateful firewall สามารถท าการติดตามสถานะของการเชื่อมต่อโดยการบันทึก เก็บไว้อยู่ในแพ็คเก็ตแต่เมื่อมองใน stateless firewall นั้นจะท าการดูทีละแพ็คเก็ต เป็นตัวๆ ไป โดยไม่รู้ว่ามีแพ็คเก็ตใดไปก่อนหน้าหรือก าลังจะมา อีกทั้ง stateful firewall นั้นมีความสามารถในการป้องกันได้ดีกว่า แต่ในเชิงประสิทธิภาพนั้น stateless firewall นั้นดีกว่า

Question 6  
ไฟร์วอลล์ประเภทใดบ้างที่พบเห็นได้ทั่วไป และข้อดีกับ ข้อเสียของประเภทเหล่านี้คืออะไร

มีไฟร์วอลล์หลายประเภท เช่น packet filtering firewalls stateful inspection firewalls application layer firewalls และ next-generation firewalls แต่ละประเภทมีจุดแข็งและจุดอ่อน องค์กร ควรประเมินความต้องการอย่างรอบคอบและเลือก ประเภทไฟร์วอลล์ที่ตรงกับความต้องการมากที่สุด

Question 7  
องค์กรจะมั่นใจในประสิทธิภาพของเครื่องมือรักษาความ ปลอดภัยได้อย่างไร และควรพิจารณาปัจจัยใดบ้างเมื่อเลือก เครื่องมือรักษาความปลอดภัยใหม

เพื่อให้มั่นใจถึงประสิทธิภาพของเครื่องมือรักษาความปลอดภัย องค์กร ควรทดสอบและประเมินสถานะการรักษาความปลอดภัยเป็นประจำผ่าน การทดสอบการเจาะระบบ การประเมินช่องโหว่ และการประเมินความ ปลอดภัยอื่นๆ พวกเขาควรตรวจสอบเครื่องมือรักษาความปลอดภัยเพื่อ หาผลบวกปลอมหรือผลลบปลอม และตรวจสอบนโยบายและขั้นตอน ความปลอดภัยเป็นประจำเพื่อให้แน่ใจว่ามีความทันสมัยและมี ประสิทธิภาพในการต่อต้านภัยคุกคามในปัจจุบัน เมื่อเลือกเครื่องมือ รักษาความปลอดภัยใหม่ องค์กรควรพิจารณาปัจจัยต่างๆ เช่น งบประมาณ ข้อกำหนดด้านความปลอดภัย การผสานรวมกับระบบที่มี อยู่ ข้อกำหนดด้านการจัดการและการบำรุงรักษา และชื่อเสียงและ ประวัติของผู้ขาย พวกเขาควรประเมินความสามารถและคุณลักษณะของ เครื่องมือรักษาความปลอดภัยต่างๆ และเลือกเครื่องมือที่เหมาะสมที่สุด กับความต้องการด้านความปลอดภัยและสภาพแวดล้อมเฉพาะของตน

Question 8  
อธิบาย antivirus software

เป็น software ที่ใช้ในการรักษาความปลอดภัยที่จะช่วยเครื่องคอมพิวเตอร์จากการ โดน virus, malware และอื่นๆ โดยการท างานจะท าการสแกนไฟล์และโปรแกรม บนเครื่องเพื่อหาสิ่งปกติและหากเจอจะท าการน าออกทันท

Question 9  
ขั้นตอนสำคัญที่เกี่ยวข้องในแผน incident response คืออะไร

แผนรับมือเหตุการณ์มักจะเกี่ยวข้องกับขั้นตอนสำคัญหลายขั้นตอน รวมถึงการเตรียมการ การระบุ การกักกัน การกำจัด การกู้คืน และ บทเรียนที่ได้รับ ในระหว่างขั้นตอนการเตรียมการ องค์กรต่างๆ จะ กำหนดนโยบายและขั้นตอนการตอบสนองต่อเหตุการณ์ ระบุผู้มีส่วนได้ ส่วนเสียและบทบาทที่สำคัญ และพัฒนาคู่มือการรับมือเหตุการณ์ ขั้นตอนการระบุเกี่ยวข้องกับการตรวจหาและจำแนกเหตุการณ์ด้าน ความปลอดภัย ในขณะที่ขั้นตอนการกักกันเกี่ยวข้องกับการแยกระบบที่ ได้รับผลกระทบและป้องกันความเสียหายเพิ่มเติม ขั้นตอนการกำจัด เกี่ยวข้องกับการลบต้นตอของเหตุการณ์ ในขณะที่ขั้นตอนการกู้คืน เกี่ยวข้องกับการคืนค่าการทำงานตามปกติและตรวจสอบให้แน่ใจว่า ข้อมูลได้รับการสำรองอย่างเหมาะสม ขั้นสุดท้าย บทเรียนที่ได้รับจะ เกี่ยวข้องกับการประเมินประสิทธิผลของincident response plan และระบุจุดที่ต้องปรับปรุง

Question 10  
องค์กรจะมั่นใจได้อย่างไรว่ากระบวนการ เผชิญเหตุมีประสิทธภาพ

เพื่อให้มั่นใจถึงประสิทธิผลของกระบวนการตอบสนองต่อเหตุการณ์ องค์กรควรทดสอบและประเมินincident response planอย่าง สม่ำเสมอผ่านการฝึกบนโต๊ะและการโจมตีจำลอง พวกเขาควรตรวจสอบ ให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งหมดได้รับการฝึกอบรมอย่างถูกต้องและ ตระหนักถึงบทบาทและความรับผิดชอบของตนในระหว่างเหตุการณ์ ด้านความปลอดภัย นอกจากนี้ องค์กรควรตรวจสอบสภาพแวดล้อมของ ตนอย่างต่อเนื่องเพื่อหาสัญญาณของเหตุการณ์ด้านความปลอดภัย และ ดูแลรักษา playbooks การตอบสนองต่อเหตุการณ์ที่เป็นปัจจุบัน ซึ่ง สะท้อนถึงข่าวกรองภัยคุกคามในปัจจุบันและแนวทางปฏิบัติที่ดีที่สุด

Question 12  
อะไรคือ Cross-site scripting และสามารถ ป้องกันได้อย่างไร

เป็นช่องโหว่ของเว็บที่อนุญาตให้มีการใส่ code ที่เป็นอันตรายลงไปในหน้าเว็บที่ผู้ใช้ รายอื่นก าลังใช้งานอยู่ สิ่งนี้ท าเพื่อขโมยข้อมูลที่มีความละเอียดอ่อนอย่าง password ในการป้องกันการโจมตีต้องมีการตรวจสอบ input ของผู้ใช้งานก่อนท าการแสดงผล หน้าเว็บ

Question 11  
ช่องโหว่ด้านความปลอดภัยบนเว็บประเภท ใดที่พบบ่อยที่สุด

ช่องโหว่ด้านความปลอดภัยของเว็บประเภททั่วไป ได้แก่ injection attacks cross-site scripting (XSS) broken authentication and session management การอ้างอิง วัตถุโดยตรงที่ไม่ปลอดภัย, การกำหนดค่าความปลอดภัย ผิดพลาด และการบันทึกและการตรวจสอบไม่เพียงพอ

Question 14  
อะไรคือ WPA2 encryption และสามารถเพิ่ม ความปลอดภัยได้อย่างไร

WPA2 ย่อมาจาก Wi-Fi Protected Access 2 ซึ่งเป็นโปรโตคอลความ ปลอดภัยที่ใช้ในเครือข่าย LAN ไร้สาย ช่วยเพิ่มความปลอดภัยโดยใช้ AES และให้การ ควบคุมความปลอดภัยที่แข็งแกร่งขึ้นส าหรับการตรวจสอบผู้ใช้WPA2 ยังใช้ keyที่ไม่ ซ้ํากันส าหรับการเชื่อมต่อแต่ละครั้งซึ่งท าให้แฮกเกอร์สามารถถอดรหัสการรับส่งข้อมูลไร้ สายและเข้าถึงเครือข่ายได้ยากขึ้น.

Question 13  
โปรโตคอลการเข้ารหัส WLAN ใดที่ ปลอดภัยที่สุด

ปัจจุบัน WPA2 เป็นโปรโตคอลการเข้ารหัส WLAN ที่ปลอดภัย ที่สุด เนื่องจากมีการเข้ารหัสที่แรงกว่าและคุณสมบัติด้านความ ปลอดภัยที่ดีกว่า WEP และ WPA อย่างไรก็ตาม สิ่งสำคัญคือ ต้องทราบว่าแม้แต่ WPA2 ก็สามารถเสี่ยงต่อการโจมตีบางอย่าง ได้ เช่น การโจมตีด้วยกำลังดุร้ายกับรหัสผ่านที่ไม่รัดกุม นอกจากนี้ องค์กรควรอัปเดตโปรโตคอลความปลอดภัย WLAN อย่างสม่ำเสมอ และตรวจสอบปัญหาด้านความปลอดภัยที่อาจ เกิดขึ้นเพื่อรักษาความปลอดภัยของ WLAN

Question 16  
Rogue access point คืออะไรและสามารถ ป้องกันได้อย่างไร

เป็น access point ที่ไม่ได้รับการยืนยันหรือทราบจากผู้ดูแลระบบ access point นี้สามารถใช้งานได้เหมือน access point ปกติแต่เมื่อเชื่อมต่อแล้วท าให้ผู้ โจมตีสามารถเข้าไปล้วงข้อมูลละเอียดอ่อนอย่าง password หรือเลขบัตรเครดิต ซึ่ง ควรใช้ระบบการป้องกันแบบไร้สาย (WIPS) ซึ่งมีความสามารถในการตรวจจับและ ป้องกัน access point ที่อยู่นอกเครือข่าย และสามารถลบ access point ที่ถูก แอบเข้ามาติดตั้งรวมทั้งระบุจุดได้ด้วย

Question 15  
ขั้นตอนแรกของกระบวนการบริหารความ เสี่ยง ตามมาตรฐาน COSO คืออะไร

การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

Question 20  
กฎหมาย PDPA คืออะไรและส่งผลต่อทางธุรกิจอย่างไร

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย ( PDPA ) เป็นกฎหมายคุ้มครอง ข้อมูลและกฎหมายความเป็นส่วนตัวที่ด าเนินการในประเทศไทยในปี 2563 บทบัญญัติที่ ส าคัญของมันรวมถึงข้อก าหนดส าหรับการได้รับความยินยอมส าหรับการประมวลผล ข้อมูลสิทธิการปกป้องข้อมูลที่เพิ่มขึ้นส าหรับบุคคลและเพิ่มความรับผิดชอบและ บทลงโทษส าหรับองค์กรที่ไม่ปฏิบัติตามกฎระเบียบ. PDPA ใช้กับทุกองค์กรที่ ประมวลผลข้อมูลส่วนบุคคลของบุคคลในประเทศไทยโดยไม่ค านึงถึงองค์กรที่เป็นฐาน. ธุรกิจที่ไม่ปฏิบัติตาม PDPA อาจต้องเสียค่าปรับจ าคุกหรือทั้งสองอย่าง.

Question 19  
พ.ร.บ.คอมพิวเตอร์ของไทยส่งผลกระทบ ต่อบริษัทต่างชาติที่ดำเนินธุรกิจในประเทศ ไทยอย่างไร?

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ของไทย มีผลบังคับใช้กับบริษัทต่างชาติที่ดำเนินธุรกิจใน ประเทศไทย และต้องรับโทษและดำเนินการบังคับเช่นเดียวกับ บริษัทไทย ซึ่งรวมถึงค่าปรับที่อาจเกิดขึ้น การจำคุก และการ ยึดระบบและข้อมูลคอมพิวเตอร์ กฎหมายดังกล่าวถูกนำมาใช้ เพื่อดำเนินคดีกับบุคคลและบริษัทต่างชาติสำหรับกิจกรรม ออนไลน์ที่ละเมิดกฎหมาย เช่น การโพสต์เนื้อหาที่ถือว่าหมิ่น ประมาทหรือวิพากษ์วิจารณ์สถาบันกษัตริย์ บริษัทต่างชาติที่ ดำเนินกิจการในประเทศไทยจึงต้องรับทราบข้อกำหนดของ CCA และตรวจสอบให้แน่ใจว่ากิจกรรมออนไลน์ของพวกเขา เป็นไปตามกฎหมาย

Question 18  
อะไรคือองค์ประกอบหลักของ ISMS ที่ สอดคล้องกับ ISO 27001 และ องค์ประกอบเหล่านี้ช่วยองค์กรในการ จัดการความเสี่ยงด้านความปลอดภัยข้อมูล

ส่วนประกอบที่สำคัญของ ISMS ที่เป็นไปตามมาตรฐาน ISO 27001 ได้แก่ การประเมินความเสี่ยง การรักษาความเสี่ยง นโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูล การ ควบคุมการเข้าถึง และการฝึกอบรมและการรับรู้ การนำ องค์ประกอบเหล่านี้ไปใช้ องค์กรสามารถสร้าง ISMS ที่มี ประสิทธิภาพซึ่งช่วยให้พวกเขาจัดการความเสี่ยงด้านความ ปลอดภัยของข้อมูลได้

Question 17  
จุดประสงค์หลักของ ISO 27001 คืออะไรและต้องทำอย่างไรถึงทำให้ได้ถึงมาตรฐานน

เป็นมาตรฐานสากลส าหรับระบบการจัดการความปลอดภัยของข้อมูล ( ISMS ) ส าหรับองค์กรในการสร้างด าเนินการบ ารุงรักษาและปรับปรุงแนวทางปฏิบัติด้านความ ปลอดภัยของข้อมูลอย่างต่อเนื่อง วัตถุประสงค์ของการรับรอง ISO 27001 คือเพื่อ แสดงให้เห็นถึงความสนใจว่าองค์กรได้ใช้ระบบการจัดการความปลอดภัยข้อมูลที่ ครอบคลุมและมีประสิทธิภาพ ในการขอรับการรับรององค์กรจะต้องได้รับการตรวจสอบ อย่างจากหน่วยงานรับรองบุคคลที่สามเพื่อตรวจสอบว่า ISMS ขององค์กรสอดคล้อง กับข้อก าหนดของมาตรฐาน ISO 27001