การเป็นมืออาชีพ ในการรักษาความปลอดภัยไซเบอร์

Become a cyber security professional

พล.ร.ต. วิศณุ สร้างวงศ์ใหม่
ผู้อำนวยการสำนักปฏิบัติการ
กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

Rear Admiral Wisnu Srangwongmai
Director of Operation Department of Communication and Information Technology RTN.
Email: siriporn.s@onec.mail.go.th

บทคัดย่อ

ในยุคข้อมูลข่าวสารปัจจุบัน ข้อมูลเป็นทรัพย์สินขององค์กร ซึ่งการประยุกต์ใช้เทคโนโลยีอย่างเหมาะสมจะช่วยเพิ่มประสิทธิภาพ มีผลให้เกิดความได้เปรียบในการแข่งขัน ในขณะที่หากข้อมูลสำคัญขององค์กรได้รับความเสียหายจะส่งผลกระทบต่อองค์กร การรักษาความปลอดภัยข้อมูลจึงมีความจำเป็นอย่างยิ่ง ด้วยการเรียนรู้กระบวนการที่จำเป็นเพื่อให้องค์กรปราศจากความเสี่ยง ลำดับขั้นของการติดตั้งอุปกรณ์ป้องกัน และภัยคุกคามที่เกิดจากเทคโนโลยี การเรียนรู้ดังกล่าวเป็นการเตรียมตัวรับมือกับเหตุที่จะเกิดขึ้น เพื่อความเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์

คำสำคัญ: ความปลอดภัยไซเบอร์, มัลแวร์, บิ๊กดาต้า, ไวรัสคอมพิวเตอร์

ABSTRACT

In the present information age Information is the property of the organisation. The application of technology is appropriate. Will help optimise this results in a competitive advantage. At the same time, if the critical information of the organisation is damaged, it will affect the organisation. Information security is essential to learning. The process required to keep the organisation free of risks. Steps of installation of protective equipment and the threat of technology. Such learning. Preparing for the incident. For professionalism in cyber security.

Keywords: Cyber Security, Malware, Big Data, Computer Virus

บทนำ

ในยุคข้อมูลข่าวสารปัจจุบัน ข้อมูลเป็นทรัพย์สินมีค่าขององค์กร และการประยุกต์ใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมจะช่วยเพิ่มประสิทธิภาพการพัฒนาองค์กร ส่งผลให้ได้เปรียบในการแข่งขัน เป็นความท้าทายขององค์กรสมัยใหม่ ในขณะที่หากข้อมูลสำคัญถูกขโมยไป ไม่สามารถใช้ได้เมื่อมีความต้องการ จะมีผลกระทบต่อองค์กรเช่นกัน อินเทอร์เน็ตเป็นเหมือนดาบสองคม ประโยชน์ที่ได้รับมีมาก อาจจะเท่ากับโทษก็ได้หากไม่รู้จักวิธีการใช้ โดยที่ไม่มีระบบใดมีความปลอดภัย 100% การรักษาความปลอดภัยข้อมูลไม่ใช่แค่การติดตั้งเทคโนโลยีที่ดีที่สุด แต่จะต้องมีการบริหารความเสี่ยง ระบุภัยคุกคาม ประเมินโอกาสที่จะเกิดขึ้น และผลกระทบเมื่อมีเหตุการณ์ต่าง ๆ เกิดขึ้น

การรักษาความปลอดภัยไซเบอร์หมายถึงกระบวนการที่จะทำให้องค์กรปราศจากความเสี่ยงและอันตรายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ไซเบอร์เป็นความหมายในเชิงนามธรรม หมายถึงขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ การใช้อุปกรณ์แท็บเล็ตและสมาร์ตโฟน รวมถึงการใช้งานเครือข่ายสังคมออนไลน์ เช่น Facebook, YouTube, Instagram หากผู้ใช้งานขาดสติแล้วพลาดเมื่อโพสต์ข้อความก็ไม่สามารถที่จะลบข้อมูลกลับคืนมาได้ ข้อมูลที่ถูกโพสต์ไปนั้นจะถูกแพร่กระจายไปเก็บไว้ในที่ต่าง ๆ บนอินเทอร์เน็ต ซึ่งข้อมูลที่ถูกจัดเก็บไว้ในโลกไซเบอร์ที่ปัจจุบันมีจำนวนมากมายมหาศาล ซึ่งรวมกันเรียกว่า Big Data ระบบเก็บข้อมูลของ Search Engine ที่ทันสมัย เช่น Google, Yahoo สามารถนำข้อมูลของเราไปวิเคราะห์ทางด้านการตลาด ทำให้เรามีโอกาสสูญเสียความเป็นส่วนตัว ซึ่งขณะนี้กำลังเป็นปัญหาใหญ่ที่ทั้งโลกจับตามอง ดังนั้น เราคงต้องระมัดระวังในเรื่องความเป็นส่วนตัวให้มากขึ้น เพราะเป็นกระแสความเปลี่ยนแปลงของโลกอนาคต

Become a cyber security professional

Become a cyber security professional เป็นชื่อหลักสูตรที่กองทัพเรือส่งข้าราชการไปเข้ารับการอบรมที่บริษัทแห่งหนึ่งในประเทศไทย ใช้เวลาประมาณ 2 วัน โดยมีวัตถุประสงค์เพื่อให้ทราบถึงแนวทางการดำเนินการจัดทำนโยบายความปลอดภัยระบบสารสนเทศที่เป็นมาตรฐานสากล รวมถึงการตรวจสอบ พร้อมทั้งดูแลระบบสารสนเทศให้เกิดความปลอดภัย ซึ่งผู้เขียนเห็นว่าจะเป็นประโยชน์สำหรับผู้บริหารองค์กรในปัจจุบันที่ต้องมีส่วนเข้าไปรับรู้ รับทราบ หรือใช้ประโยชน์จากระบบสารสนเทศ ไม่ว่าจะโดยตรงหรือทางอ้อม หรือแม้แต่ผู้ใช้งานโทรศัพท์สมาร์ตโฟนโดยทั่วไป หากมีความเข้าใจเกี่ยวกับการรักษาความปลอดภัยในโลกไซเบอร์จะทำให้ไม่ตกเป็นเหยื่อของผู้ไม่ประสงค์ดีที่แฝงตัวเข้ามาในรูปแบบต่าง ๆ ผ่านโทรศัพท์มือถือที่ใช้อยู่ทุกวัน โดยในหลักสูตรจะกล่าวถึง Cyber Security Concept เรียนรู้ถึงกระบวนการ หรือการกระทำทั้งหมดที่จำเป็นเพื่อให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ Security Architecture Principles เรียนรู้เกี่ยวกับลำดับชั้นของเน็ตเวิร์กและอุปกรณ์ การติดตั้งอุปกรณ์ป้องกันการบุกรุก เช่น Firewalls หรือโปรแกรมประยุกต์ เช่น Antivirus Security of Network, System, Application and Data เรียนรู้เกี่ยวกับหลักเกณฑ์และจัดการกับความเสี่ยงที่จะเกิดขึ้นโดยใช้เครื่องมือต่าง ๆ และสุดท้ายได้แก่ Security Implication and Acceptation of Evolving Technology

เรียนรู้เกี่ยวกับภัยคุกคามที่จะเกิดจากเทคโนโลยี เช่น Mobile, Internet of Thing

1. Cyber Security Concept

กระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูลการระวังป้องกันอาชญากรรม การโจมตี การบ่อนทำลาย การโจรกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ ซึ่งยังรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้มีผลประโยชน์ร่วม มีสิ่งสำคัญที่ต้องทราบ 3 ประการ ได้แก่ Confidentiality หรือคุณสมบัติของการควบคุมและการอนุญาตให้เข้าถึง หรือเปิดเผยข้อมูล รวมถึงการป้องกันข้อมูลส่วนบุคคล Integrity หรือคุณสมบัติของการปกป้องข้อมูล และระบบจากการดัดแปลงหรือทำลายโดยไม่สมควร รวมไปถึงการยืนยันตัวบุคคลหรือที่มา และ Availability หรือคุณสมบัติของข้อมูลและระบบที่จะต้องพร้อมใช้งานและเข้าถึง ได้อย่างรวดเร็ว ซึ่งเมื่อองค์กรได้ดำเนินการหลักการทั้ง 3 ประการขั้นต้นแล้ว ต่อไปเรียกว่าขั้นตอนการทำ Cyber Security เพื่อให้เกิดความปลอดภัยของข้อมูลสอดคล้องกับวัฒนธรรมองค์กร การจัดทำนโยบายไม่สามารถหาได้จากเอกสารมาตรฐานข้อกำหนดทั่วไปที่ใช้มาแล้วประสบความสำเร็จ เนื่องจากแต่ละองค์กรมีวัตถุประสงค์ต่างกัน แต่พอสรุปได้ว่านโยบายที่ดีควรมีขอบเขตแน่ชัด มีผลบังคับใช้ ปฏิบัติได้จริง เข้าใจง่ายไม่ซับซ้อน หรือรวบรัดจนเกินไป เนื้อหาไม่ขัดแย้งกันเอง และจะต้องปรับปรุงหรือทบทวนอยู่เสมอ มีเวอร์ชั่นกำกับทุกครั้งที่มีการแก้ไข

ภัยคุกคามทางไซเบอร์สามารถแบ่งออกเป็นกลุ่มต่าง ๆ ได้ 4 กลุ่ม ได้แก่

1) ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์โทรศัพท์เคลื่อนที่ และแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่ามัลแวร์ ซึ่งถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ที่ทำให้เกิดการขัดข้อง เสียหายกับระบบปฏิบัติการ นอกจากนี้สามารถส่งข้อความไม่พึงประสงค์ออกไปยังที่อื่น ขโมยข้อมูลสำคัญออกไป ตัวอย่างของโปรแกรมเหล่านี้ ได้แก่ Virus, Worm, Trojan, Botnets

มัลแวร์ที่แบ่งตามวิธีการกระจายตัว

Virus เป็นมัลแวร์ที่ฝังอยู่ในโปรแกรมทำงาน เมื่อโปรแกรมถูกรันการแพร่กระจายต้องอาศัย User Action ก่อนจึงจะกระจายตัวได้

Trojan เป็นมัลแวร์ที่แฝงอยู่ในเครื่องเพื่อรอดำเนินการบางอย่าง แพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือแฝงมากับโปรแกรมต่าง ๆ เช่น โปรแกรมฟังเพลง

Worm เป็นมัลแวร์ที่ทำงานเอง ยูสเซอร์ไม่ต้องทำอะไร แพร่ผ่านทางเน็ตเวิร์ก หรือช่องเสียบ USB

มัลแวร์ที่แบ่งตามการกระทำต่อระบบ

Spyware จุดประสงค์เพื่อสอดแนมข้อมูลบางอย่าง เช่น รหัสผ่าน บัญชีการเงิน ลำดับการกดคีย์บอร์ด

Rootkit เป็นมัลแวร์ที่จะยกระดับให้ผู้ใช้สามารถมีสิทธิ์ต่าง ๆ เหมือนแอดมินของระบบ สามารถเข้าถึงสิทธิ์ของแอดมินแล้วไปเปลี่ยนฟังก์ชันของระบบให้ตรวจไม่พบมัลแวร์นั้น ๆ

Botnet คือเครือข่ายคอมพิวเตอร์ที่ถูกมัลแวร์ฝังตัวอยู่ในเครื่องเพื่อใช้พลังการประมวลผลของเครื่องไปทำกิจกรรมบางอย่าง เช่น การโจมตีประเภท DDoS, การขุด Bitcoin ซึ่งเมื่อเครือข่ายถูก Botnet โจมตีเครื่องจะตกอยู่ในสภาพที่เรียกว่าซอมบี้ ช้าอืดอาดไม่สามารถทำงานได้

Ransomware คือซอฟต์แวร์เรียกค่าไถ่ที่จะล็อกเครื่องไม่ให้ใช้งานได้จนกว่าจะจ่ายเงิน

2) ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ถูกออกแบบมาให้เหมือนของจริง หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์ เฟซบุ๊ก หรือเว็บไซต์ทางการเงิน แล้วดักจับรหัส

ของผู้ใช้งาน ทำให้ข้อมูลหรือบัญชีนั้น ๆ มีความเสี่ยงไม่ปลอดภัย

3) ภัยคุกคามจากการใช้เครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกัน โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สายหรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญหรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4) ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน วิกฤตสถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐและภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2. Security Architecture Principles

องค์กรมาตรฐานระหว่างประเทศได้พัฒนาโมเดลของการทำงานบนระบบเครือข่ายที่เป็นมาตรฐานกลางที่ผู้ผลิตอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์จะต้องมีมาตรฐานตามที่กำหนด แบ่งออกเป็น 7 ลำดับชั้น ได้แก่

1. Physical Layer เป็นชั้นล่างสุด เป็นการกำหนดคุณสมบัติทางกายภาพของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่างคอมพิวเตอร์

2. Data Link Layer กำหนดรูปแบบของการส่งข้อมูลข้ามเน็ตเวิร์ก

3. Network Layer ทำหน้าที่ส่งข้อมูลข้ามเครือข่าย

4. Transport Layer ทำหน้าที่เชื่อมต่อกับ Upper Layer

5. Session Layer ทำหน้าที่ควบคุมการเชื่อมต่อ

6. Presentation Layer ทำหน้าที่นำเอาข้อมูลที่ต้นทางให้สามารถสื่อสารกับปลายทางได้

7. Application Layer ทำหน้าที่ติดต่อระหว่างยูสเซอร์กับแอพพลิเคชั่น

ในระบบเครือข่ายที่มีผู้ใช้งานจำนวนมาก มีทั้งผู้ประสงค์ดีและประสงค์ร้าย พวกที่คอยดักจับสัญญาณโดยใช้เครื่องมือพิเศษแอบบันทึกข้อมูล เช่น Hacker หรือ Virus Computer ซึ่งโปรแกรมเมอร์เขียนขึ้นมาเพื่อจุดประสงค์บางประการ ส่วนการป้องกันเครือข่ายก็มีหลายวิธีเช่นกัน ได้แก่

- Firewall ทำหน้าที่ควบคุมทราฟฟิกที่เข้าสู่เน็ตเวิร์ก มีการกำหนดนโยบายในการผ่านเข้าออก และสามารถป้องกันการโจมตีแบบ DDoS ที่ทำให้เน็ตเวิร์กล่มโดยการทำทราฟฟิกปลอม

- Intrusion Prevention System (IPS) ทำหน้าที่ตรวจจับและป้องกันการโจมตีจาก Hacker, Virus, Worm ที่ผ่านเข้ามาในระบบ

- Gateway Antivirus ตรวจจับภัยคุกคามที่มากับคอนเทนต์ของเว็บไซต์ในลักษณะเรียลไทม์

- Web Jittering ป้องกันการเข้าเว็บไซต์ที่ไม่ปลอดภัยหรือผิดกฎหมาย

- การเก็บล็อกข้อมูลการจราจรทางคอมพิวเตอร์เพื่อตรวจสอบย้อนกลับ

- การระมัดระวังการใช้งาน ไม่ใช้แผ่นดิสก์ร่วมกับผู้อื่น โหลดไฟล์จากอินเทอร์เน็ตซึ่งมีโอกาสติดไวรัสสูง

- หมั่นสำเนาข้อมูลอยู่เสมอ เป็นการป้องกันข้อมูลเสียหาย

- ติดตั้ง Firewall ป้องกันการบุกรุกจากผู้ไม่ประสงค์ดี

- การทำฮาร์ดเดนนิ่งป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันการบุกรุกจากแฮกเกอร์ ลดสิ่งที่ไม่ได้ใช้ออกจากระบบ

- การใช้รหัสผ่าน ควรมีการเปลี่ยนรหัสบ่อย ๆ เป็นระยะ

3. Security Implications and Adoption of Evolving Technology

APT (Advanced Persistent Threats) เป็นการโจมตีระบบเครือข่ายรูปแบบหนึ่งที่แฮกเกอร์จะเลือกเป้าหมายเพียงรายเดียว แล้วมุ่งโจมตีเฉพาะเป้าหมายนั้น โดยอาศัยเทคนิคการโจมตีรูปแบบต่าง ๆ ผสานกันเพื่อให้ประสบผลสำเร็จ ไม่ว่าจะเป็นการทำ Social Engineering อาศัยข้อมูลของเป้าหมายที่รวบรวมมาได้ หรือการออกแบบมัลแวร์สำหรับใช้โจมตีเป้าหมายโดยเฉพาะ เป็นต้น กระบวนการโจมตี แทรกซึม ลบร่องรอย และขโมยข้อมูล อาจกินเวลาตั้งแต่หลักสัปดาห์ไปจนถึงหลักปีเลยทีเดียว เนื่องจาก ATP เป็นการโจมตีที่ออกแบบมาเฉพาะกับเป้าหมายนั้น ๆ ทำให้ระบบรักษาความมั่นคงปลอดภัยทั่วไปอาจไม่สามารถรับมือกับชุดการโจมตีที่ประกอบไปด้วย Zero-day Exploits, Phishing, Advanced Malware และ Web Attacks หลากหลายรูปแบบได้ เพื่อเสริมความแข็งแกร่งให้กับระบบขององค์กร ผู้ดูแลระบบ IT Security ควรพิจารณาถึง การออกแบบระบบความมั่นคงปลอดภัยแบบ Defense in Depth ติดตั้งระบบตรวจจับและเฝ้าระวังที่มีประสิทธิภาพ ใช้บริการ Threat Intelligence จัดอบรมเพื่อเพิ่มความตระหนักรู้ทางด้านความมั่งคงปลอดภัยและวางแผนสำหรับรับมือกับเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น

การใช้เทคโนโลยีสำหรับผู้ใช้ที่แพร่หลายในองค์กรกำลังเปลี่ยนรูปแบบอุปกรณ์ปลายทางขององค์กร นั่นคือข้อมูลองค์กรสามารถเข้าถึงได้ผ่านทางอุปกรณ์มือถือที่บริษัทไม่ได้เป็นเจ้าของ หรือไม่ได้รับการดูแลด้านความปลอดภัยโดยฝ่ายไอทีขององค์กร ซึ่งมีแนวโน้มที่จะนำไปสู่การละเมิดความปลอดภัยหรือการสูญเสียข้อมูลที่เพิ่มสูงขึ้นอย่างมาก ปัจจุบันมีเทคโนโลยีซึ่งเป็นที่สนใจของคนทั่วไปคือ Internet of Things หรือ IoT หมายถึงการที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งอย่างสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถควบคุมการใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การเปิด-ปิดอุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องมือทางการเกษตร อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต โมบิลนั้นมีคุณสมบัติที่เหมาะต่อการโจมตีอย่างมาก ทำให้มีรูปแบบการโจมตีที่หลากหลายทั้งจากการโจมตีที่คนใช้งาน ทั้งจากการโจมตีที่โมบิล ซึ่งมีหลายแพลตฟอร์ม เช่น Android, iOS และ Windows Phone ทั้งจากการโจมตีผ่านแอพ ซึ่งผู้พัฒนาไม่ใส่ใจ หรือไม่รู้ เช่น การจัดเก็บข้อมูลที่สำคัญโดยไม่เข้ารหัสอะไรเลย ทั้งจากการโจมตีผ่านระบบเน็ตเวิร์กที่ไม่ปลอดภัยและอื่นๆ

แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์มีความรุนแรงมากขึ้น ไม่ว่าจะเป็นการที่ผู้ไม่หวังดีโจมตีช่องโหว่ของผลิตภัณฑ์ที่ถูกยุติการให้บริการสนับสนุนไปแล้ว มัลแวร์ที่มีความซับซ้อนและมีความสามารถในการหลบหลีกการตรวจจับมากขึ้น รวมถึงภัยคุกคามที่เกี่ยวกับโทรศัพท์มือถือจะพบเห็นได้มากขึ้น ในขณะที่รูปแบบการโจมตีผู้ใช้ทั่วไป องค์กร และระบบสารสนเทศต่าง ๆ อาจมีการเปลี่ยนแปลงทั้งในเชิงกระบวนการและเทคนิค และเรื่องการสอดแนมข้อมูล ก็ทำให้ทุกคนต้องเรียนรู้

สรุป

องค์กรสมัยใหม่ทั้งรัฐและเอกชนต่างก็อาศัยเทคโนโลยีสารสนเทศเพื่อสนับสนุนการปฏิบัติงานให้ประสบความสำเร็จ แต่ระบบสารสนเทศมีความซับซ้อน มีตั้งแต่ระบบบัญชี การเงิน บุคลากร หรือระบบควบคุมการอุตสาหกรรม ระบบอาวุธ ระบบดังกล่าวมีความเสี่ยงในการได้รับความเสียหาย จึงจำเป็นที่ผู้บริหารทุกระดับต้องตระหนักถึงความสำคัญ การรักษาความปลอดภัยข้อมูล เป็นกระบวนการในเชิงรุกเพื่อบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ แต่ส่วนใหญ่องค์กรจะรอให้เกิดเหตุการณ์ขึ้นก่อนแล้วค่อยหาวิธีป้องกัน ซึ่งจะมีค่าใช้จ่ายมากกว่าความเสียหายที่เกิดขึ้น อย่างไรก็ตาม การวางแผนเพื่อเตรียมรับมือกับเหตุการณ์และการบริหารความเสี่ยงจะทำให้ค่าความเสียหายลดลง หรืออาจไม่เกิดเหตุการณ์นั้น ๆ เลย เนื่องจากมีการป้องกันไว้แล้ว บทความ Become a cyber security professional คงไม่ยากเกินจะทำความเข้าใจสำหรับท่านผู้บริหารองค์กรทั้งหลาย และคงเป็นประโยชน์สำหรับการตัดสินใจในการรักษาความปลอดภัยข้อมูลขององค์กร หรือของตัวท่านผู้บริหารเอง