

แนวโน้มและภัยคุกคามด้านเทคโนโลยีสารสนเทศ

นาวาเอก ศุภเศรษฐ์ ศิริสังข์ไชย ร.น.
ผู้อำนวยการกองบรรณสารและเทคโนโลยีสารสนเทศ
กองบัญชาการสถาบันวิชาการป้องกันประเทศ

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทในชีวิตประจำวันของเรามากขึ้นเรื่อย ๆ จนแทบจะกลายเป็นส่วนหนึ่งของชีวิต ช่วงเวลาไม่กี่ปีที่ผ่านมามีการเปลี่ยนแปลงอย่างรวดเร็วและต่อเนื่องจนตามแทบไม่ทัน ส่งผลกระทบต่อการทำงานและการใช้ชีวิตประจำวัน มีการนำเทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ตมาใช้ในกระบวนการทำงานมากขึ้น การจัดเก็บและแลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานทำให้เกิดแนวโน้มการกระทำผิดเกี่ยวกับข้อมูลข่าวสารเพิ่มขึ้น

ภัยที่เกิดจากการเข้าถึงโดยมิชอบ ซึ่งระบบหรือข้อมูลคอมพิวเตอร์ รวมทั้งการโจมตีต่อระบบรักษาความปลอดภัยด้านข้อมูลข่าวสาร มีการพัฒนา เปลี่ยนแปลงรูปแบบวิธีการอยู่ตลอดเวลา รวมทั้งมีการปกปิด

อำพรางยากต่อการตรวจพบ และนับวันจะทวีความรุนแรงและสลับซับซ้อนมากขึ้น ส่งผลกระทบต่อความมั่นคงของชาติโดยรวม การศึกษาและทำความเข้าใจถึงกระแสและแนวโน้มของเทคโนโลยีสารสนเทศจะช่วยให้สามารถเตรียมการเพื่อรับมือกับภัยคุกคามที่จะเกิดขึ้นในรูปแบบต่าง ๆ สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

แนวโน้มเทคโนโลยีสารสนเทศ

แนวโน้มเทคโนโลยีปี พ.ศ. ๒๕๕๖ โดยการ์ดเนอร์ ในแต่ละปี บริษัทที่ปรึกษาและวิจัยชั้นนำด้านไอทีของโลกที่ชื่อว่า การ์ดเนอร์ (Gartner) จะทำนายหรือพยากรณ์เทคโนโลยีระดับยุทธศาสตร์ซึ่งเป็นเทคโนโลยีที่มีความสำคัญ และมีผลกระทบต่อองค์กรอย่างมากในระยะเวลา ๓ ปีข้างหน้า ทั้งนี้เพื่อให้ผู้บริหารได้พิจารณานำเอาเทคโนโลยีเหล่านี้มาใช้ มิฉะนั้นแล้วองค์กรอาจก้าวไปข้างหน้าได้อย่างล่าช้าไม่ทันกับการเปลี่ยนแปลงที่รวดเร็ว สำหรับปี พ.ศ. ๒๕๕๖ นั้น จะเป็นการหลอมรวมระบบของเทคโนโลยีสื่อสังคม (Social Networks) เทคโนโลยีพกพา เทคโนโลยีคอมพิวเตอร์แบบคลาวด์ และเทคโนโลยีสารสนเทศ ซึ่งมี ๑๐ เรื่อง ดังนี้

๑. อุปกรณ์พกพา (Mobile Device Battles) ในปี พ.ศ. ๒๕๕๖ อุปกรณ์พกพาจะมีจำนวนมากกว่า



คอมพิวเตอร์ส่วนบุคคล ในการใช้เป็นอุปกรณ์เข้าถึงเว็บ ในปี พ.ศ. ๒๕๕๘ อุปกรณ์โทรศัพท์ที่ขายในตลาดจะเป็นสมาร์ทโฟน (Smart Phone) เป็นจำนวนมากถึง ๘๐% และในจำนวนนี้มีเพียง ๒๐% เท่านั้นที่จะเป็นวินโดวส์โฟน (Windows Phone) ในปีเดียวกันนี้ แท็บเล็ตจะขยายตลาดไปถึง ๕๐% ของตลาดโน้ตบุ๊ก ในที่สุดองค์กรก็จะใช้อุปกรณ์หลากหลายที่ใช้ระบบปฏิบัติการหลัก เรียงลำดับดังนี้ แอนดรอยด์ (Android) ของกูเกิล (Google) ไอโอเอส (iOS) ของแอปเปิล (Apple) และวินโดวส์ ๘ (Windows 8) ซึ่งมีส่วนแบ่งเพียงแค่อันดับสามเท่านั้น แสดงให้เห็นว่าระบบปฏิบัติการวินโดวส์ไม่ได้เป็นระบบปฏิบัติการหลักอีกต่อไป ความหลากหลายของการใช้อุปกรณ์การสื่อสารแบบพกพาเช่นนี้ ทำให้องค์กรต้องตระหนักถึงการเตรียมพร้อมโครงสร้างพื้นฐานระบบไอทีในองค์กรที่รองรับความหลากหลายเหล่านี้ให้ได้

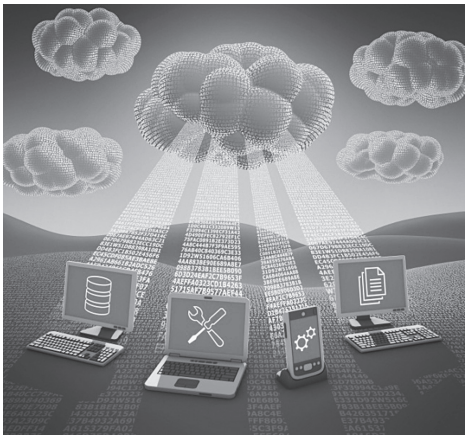
๒. แอพพลิเคชันโมบายล์และ HTML5 (Mobile Applications and HTML5)

จะพบว่าตลาดเครื่องมือพัฒนาแอปพลิเคชันจะมีความซับซ้อนมากขึ้น เนื่องจากมีบริษัทผลิตเครื่องมือมากกว่า ๑๐๐ แห่ง ทั้งนี้ การทำนายของการ์ดเนอร์บอกว่ามีการแบ่งแยกเครื่องมือพัฒนาแอปพลิเคชันบนอุปกรณ์พกพาออกเป็นหลายประเภท ดังนั้น จึงเป็นการยากที่บริษัทใดบริษัทหนึ่งจะสามารถพัฒนาแอปพลิเคชันเดียวให้รองรับกับทุกอุปกรณ์ได้ องค์กรคงหลีกเลี่ยงไม่ได้ที่จะต้องใช้เครื่องมือพัฒนาแอปพลิเคชันที่หลากหลายเครื่องมือที่ใช้จะเป็นเครื่องมือเฉพาะทางตามสถาปัตยกรรมของแอปพลิเคชันที่ยังนิยมใช้อยู่ อาทิ แบบเนทีฟ (Native) ซึ่งเป็นแอปพลิเคชันที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์และถูกออกแบบมาให้ทำงานอยู่ในระบบปฏิบัติการที่กำหนด แบบพิเศษ (Special) แบบผสม (Hybrid) แบบ HTML5 แบบ Message และแบบ No Client เป็นต้น การพัฒนาแอปพลิเคชันจะเริ่มมาเน้นการสร้างด้วย HTML5

แทนที่จะเป็นแบบเนทีฟ เนื่องจากความสามารถของ HTML5 ที่เพิ่มมากขึ้นนั่นเอง อย่างไรก็ตาม แอปพลิเคชันที่ยังยืนหยัดได้อย่างชัดเจนหรือแน่ ๆ ว่าไม่หายไปไหนก็คงเป็นสถาปัตยกรรมแบบเนทีฟ นักพัฒนาจะต้องเรียนรู้และเพิ่มทักษะการพัฒนาแอปพลิเคชันที่อยู่ในอุปกรณ์ต่าง ๆ ที่สามารถทำงานประสานกันได้

๓. คลาวด์ส่วนตัว (Personal Cloud)

คลาวด์ส่วนตัวเป็นคอมพิวเตอร์เชิงอุปกรณ์ที่ใช้เก็บข้อมูลส่วนตัว แทนที่จะใช้คอมพิวเตอร์ส่วนบุคคล และเป็นจุดศูนย์กลางในการทำกิจกรรม



ชีวิตดิจิทัลของประชาชน เมื่อทุกคนใช้อุปกรณ์อิเล็กทรอนิกส์ในรูปแบบต่าง ๆ ในการเข้าถึงข้อมูลและการบริการในระหว่างที่ดำเนินชีวิตประจำวัน การทำธุรกิจหรือการทำธุรกรรมต่าง ๆ ล้วนต้องต่อเชื่อมกับคลาวด์ส่วนตัว ซึ่งมีสภาพพร้อมใช้งานได้ในทุกที่ทุกเวลา ดังนั้นแนวคิดจึงเปลี่ยนไปเป็นการเน้นที่บริการที่ใช้กับอุปกรณ์ใด ๆ ก็ได้

๔. แอปสโตร์ขององค์กร (Enterprise App Stores)

แอปสโตร์จะมีความซับซ้อน องค์กรต่าง ๆ เริ่มต้องซื้อแอปของผู้จำหน่ายหลากหลาย โดยมีเงื่อนไขการขายอยู่ในแอปสโตร์ ซึ่งส่งผลให้มีความยุ่งยากมากในด้านลิขสิทธิ์ การซ่อมบำรุง ดังนั้น ในปี พ.ศ. ๒๕๕๗ การ์ดเนอร์ได้ทำนายว่าองค์กรจะมีแอปสโตร์ส่วนตัวในการให้พนักงานโหลดแอปสโตร์ไปใช้ เพราะองค์กรเองก็จะเจรจากับผู้ผลิตในการให้เป็นซับพลายหรืออุปทานขององค์กร

๕. อินเทอร์เน็ต ออฟ ธิงส์ (The Internet of Things) Internet of Thing (IoT) หรือ อินเทอร์เน็ต ออฟ ธิงส์ เป็นคำพูดที่สื่อสารถึงการแพร่ขยายของอินเทอร์เน็ตไปในอุปกรณ์ต่าง ๆ ไม่ว่าจะเป็นเครื่องใช้ไฟฟ้าอิเล็กทรอนิกส์ อุปกรณ์เซ็นเซอร์ ระบบชำระเงิน เช่น การเชื่อมต่อสัญญาณและถ่ายโอนข้อมูลในระยะใกล้ (Near Field Communication หรือ NFC) อุปกรณ์พกพาจะได้นำไปใช้ในบริการและอุตสาหกรรมต่าง ๆ อาทิ เภสัชภัณฑ์ รถยนต์ นาฬิกา โปสเตอร์อัจฉริยะ โทรทัศน์ วิทยุ ฯลฯ โดยที่ทั้งหมดนี้จะมีการเชื่อมต่อกับอินเทอร์เน็ต ซึ่งจะส่งผลให้เกิดแอปพลิเคชันใหม่ ๆ และสิ่งท้าทายอื่น ๆ ที่ตามมาอย่างมากมาย

๖. ไอทีพันธุ์ผสม และคอมพิวเตอร์แบบคลาวด์ (Hybrid IT and Cloud Computing)

ในขณะที่หน่วยงานไอทีขององค์กรต้องเริ่มประหยัดงบประมาณ หน่วยงานไอทีจึงต้องมีการดำเนินงานในเชิงรุกในการประสานงานการใช้อุปกรณ์ไอทีอย่างคุ้มค่า อย่างไรก็ดี จากการสำรวจของส่วนให้บริการด้านไอทีของบริษัทวิจัย การ์ดเนอร์ พบว่าตัวแทนซื้อขายบริการคลาวด์ในองค์กร หรือ Cloud Services Brokerage (CSB) ได้มีความสำคัญมากและจะมีหน้าที่สำคัญคือต้องรับผิดชอบในการที่จะช่วยเตรียมการ จัดหา และปรับปรุงกระบวนการภายในองค์กรเพื่อให้มีความพร้อมและเกิดการใช้ระบบคลาวด์สำหรับภายในองค์กรเองและพันธมิตรธุรกิจภายนอกบริษัทด้วย ทั้งนี้เพื่อให้หน่วยงานสามารถ

สร้างมูลค่าเพิ่มและใช้คลาวด์ในการให้บริการแก่ลูกค้าเพิ่มมากขึ้น

๗. ข้อมูลมหึมา (Strategic Big Data)

ข้อมูลจะมีผลต่อองค์กร ขนาดข้อมูล ความหลากหลายของข้อมูล ความเร็ว และความซับซ้อนที่เกิดขึ้นจะมีผลต่อสถาปัตยกรรมสารสนเทศขององค์กร นอกจากนั้น ข้อมูลขนาดมหึมาได้ส่งผลให้มีการเปลี่ยนแปลงวิธีการบริการจากแบบเดิม ๆ ที่ใช้คลังข้อมูลเดียว แนวโน้มนี้คือองค์กรจะใช้ระบบหลายระบบที่ประกอบด้วย ระบบบริการเนื้อหา ระบบคลังข้อมูล คลังข้อมูลย่อย (Data Mart) และ ระบบแฟ้มข้อมูลพิเศษ (Specialized File Systems) ที่ผูกติดอยู่กับเมตาดาตา และดาตาเซอร์วิส ซึ่งจะเป็นคลังข้อมูลเชิงตรรกะขององค์กร (Logical Enterprise)

๘. แอกชันเนเบิลอนาลิติก (Actionable Analytics)

อนาลิติก คือการวิเคราะห์พฤติกรรมของผู้ใช้ในบริบทต่าง ๆ ซึ่งจะมีผลต่อประสิทธิภาพและค่าใช้จ่ายด้านไอที ดังนั้นแนวโน้มคือ อนาลิติกสามารถนำไปใช้ในส่วนตัดสินใจได้ทันที อุปกรณ์พกพาที่ต้องเชื่อมกับระบบคลาวด์ที่มีบริการการทำนายผล หรือการจำลองเหตุการณ์ ส่วนมากการวิเคราะห์จะส่งผลให้ผู้ใช้มีข้อมูลทันที ณ จุดที่ต้องใช้ ดังนั้นทุกกระบวนการทางธุรกิจที่ต้องการการตัดสินใจอย่างทันท่วงทีจะมีข้อมูล และคำแนะนำที่สามารถเลือกมาช่วยในการวินิจฉัยและตัดสินใจได้

๙. การประมวลผลในหน่วยความจำ (In Memory Computing)

การคำนวณหรือการประมวลผลในหน่วยความจำ หรือ In Memory Computing (IMC) นี้ สามารถทำให้งานหรือการคำนวณที่ต้องใช้เวลามาก โดยให้ใช้เวลาเพียงเสี้ยววินาทีเท่านั้นเอง เนื่องจากความสามารถที่ทำงานพร้อมกันได้หลายแอปพลิเคชันในเวลาเดียวกัน ดังนั้นโอกาสที่จะคำนวณหาความสัมพันธ์ของข้อมูลเพื่อหาความเป็นไปได้ของเรื่องต่าง ๆ ที่จะใช้ก็ย่อมเป็นไปได้ อย่างไรก็ดี คงไม่นานเกินรอ บริษัทการ์ดเนอร์ยังทำนายว่าภายในเวลา ๒ ปีนับจากนี้จะเกิดสิ่งเหล่านี้ขึ้นอย่างแน่นอน นั่นคือจะมีผลทำให้มีบริษัทจำนวนมากที่จะสร้างแอปพลิเคชันเป็น IMC นอกจากนั้น ยังเป็นโอกาสให้องค์กรสร้างนวัตกรรมในการทำงานได้

๑๐. ระบบนิเวศแบบบูรณาการ (Integrated Ecosystems)

เนื่องจากผู้ใช้ได้คำนึงถึงประสิทธิภาพการทำงานของระบบ อาทิ ใช้งานง่าย ค่าใช้จ่ายต่ำ และมีความมั่นคงปลอดภัยสูง ประกอบกับตลาดกำลังปรับไปสู่ระบบแบบบูรณาการและระบบนิเวศเข้าด้วยกัน ทั้งนี้จะมีผลให้องค์กรเริ่มขยับจากระบบที่มีความหลากหลายซึ่งต่อเชื่อมกันแบบไม่แน่นแฟ้นนักมาเป็นแบบบูรณาการ และเป็นระบบนิเวศที่ทำให้แอปพลิเคชันและอุปกรณ์ต่าง ๆ สามารถทำงานร่วมกันได้ โดยที่การบูรณาการจะเกิดขึ้นใน ๓ ระดับด้วยกันคือ ๑. เครื่องใช้ (Appliance) ต่าง ๆ ที่ประกอบไปด้วยฮาร์ดแวร์และซอฟต์แวร์ ๒. ซอฟต์แวร์และบริการที่รวมเข้าไว้ด้วยกัน และ ๓. โครงสร้างพื้นฐานหรือแอปพลิเคชันเวิร์กโหลด

แนวโน้มเทคโนโลยีปี พ.ศ. ๒๕๕๖ โดย พีท แคชมอร์ ซีอีโอและผู้ก่อตั้งบริษัทที่เกี่ยวข้องกับวิวัฒนาการด้านเทคโนโลยี MASHABLE ได้แก่

๑. การประมวลผลแบบสัมผัส รูปแบบวิธีการป้อนข้อมูลใหม่จะเป็นเทรนด์ที่ได้รับความสนใจอย่างมากในปี พ.ศ. ๒๕๕๖ คอมพิวเตอร์แท็บเล็ต เช่น iPad จะเป็นทางเลือกแทนคอมพิวเตอร์ตั้งโต๊ะและโน้ตบุ๊ก เนื่องจากรูปลักษณ์ที่กะทัดรัดสามารถพกพาได้ง่าย

กว่า ทำให้มีคนเลือกมาใช้แทนคอมพิวเตอร์เดิม ดังนั้น Mouse ที่ใช้อยู่กันปัจจุบันนี้ก็จะถูกแทนที่ด้วยระบบสัมผัสแทน สัญญาณที่เห็นเด่นชัดก็คือ ระบบปฏิบัติการล่าสุดอย่าง Window 8 และ Mac OS X Lion เริ่มนำเทคโนโลยีระบบสัมผัสมาใช้ควบคู่กับ OS ดังกล่าว



๒. สัญญาณทางสังคม ในโลกสื่อสังคมออนไลน์ปัจจุบัน รูปแบบสังคมที่ปรากฏอยู่ตอนนี้จะเป็นตัวชี้ให้เห็นถึงแนวทางในปี พ.ศ. ๒๕๕๖ จากข้อมูลของ facebook ปีที่แล้ว ได้เกิดสิ่งที่เรียกว่า “frictionless sharing” เป็นรูปแบบการแบ่งปันข้อมูลข่าวสารต่าง ๆ เช่น รูปภาพ สถานะความคิดเห็น วิดีโอหรือข่าวต่าง ๆ โดยการโพสต์หรือแบ่งปันให้เพื่อนที่ยังไม่เคยเห็นหรืออ่านมาก่อนได้รับข้อมูลหรือเพลิดเพลินกับสิ่งที่แชร์ไป ซึ่งทุกอย่างที่เราฟัง อ่านหรือดูจะถูกโพสต์ในหน้าเพจของเราอัตโนมัติหลังจากที่เราได้ยืนยันกับแอปพลิเคชันดังกล่าวแล้ว แนวโน้มนี้ได้รับการตอบรับที่ดีในสังคมโลกออนไลน์ ปัจจุบันมีผู้สมัครใช้งาน facebook แล้วมากกว่า ๘๐๐ ล้านคน

๓. NFC และการจับจ่ายผ่านทางมือถือ การริเริ่มการใช้จ่ายผ่านทางมือถือ รวมไปถึงระบบ NFC (Near Field Communication) ที่จะเข้ามาแทนที่การใช้จ่ายผ่านบัตรเครดิต เพียงแค่นำมือถือที่รองรับระบบ NFC มาสแกนที่เครื่องรูดบัตรในร้านค้าก็จะทำการหักเงินจากบัญชีของผู้ใช้ในทันที

๔. Kindle Fire แทนที่ iPad ในปี พ.ศ. ๒๕๕๖ iPad มีคู่แข่งที่เข้ามาสู่ตลาดแท็บเล็ต คือ Kindle Fire จาก Amazon สาเหตุที่ทำให้ iPad เสียเปรียบกว่า คือ เรื่องราคา เพราะ Kindle Fire มีราคาเพียง $199 โดยที่ iPad มีราคาสูงถึง $499 เหตุผลถัดมา คือ Amazon ยังมีจุดขายสำคัญเรื่องโปรแกรมต่าง ๆ ทั้งดูหนัง ทีวีโชว์ e-Book และอื่น ๆ อีกมากมาย ซึ่งเทียบได้ใกล้เคียงกับ iPad ปัจจุบัน Amazon ยังไม่ยืนยันเรื่องระบบปฏิบัติการว่าจะใช้ Android หรือใช้แพลตฟอร์มใหม่

๕. ทีวีทุกที่ ตอนนี้บริษัทผู้ให้บริการเคเบิลทีวีทั้งหลายกำลังเริ่มหาและวางกลยุทธ์เพื่อแก้ปัญหารายได้ที่ลดลง โดยจะให้บริการเคเบิลผ่านอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ ทำให้ลูกค้าสามารถชมรายการถ่ายทอดสด ภาพยนตร์ หรือทีวีโชว์ได้ทุกที่ เพียงแค่สมัครเป็นสมาชิกเท่านั้นเอง ขณะนี้มีผู้ให้บริการแบบนี้แล้วคือ Time Warner และ Comcast นอกจากนี้โทรทัศน์แบบพกพาเริ่มมีเพิ่มมากขึ้นควบคู่ไปกับการเติบโตของแท็บเล็ต

๖. การสั่งงานผ่านระบบเสียง Siri โปรแกรมที่สั่งงานผ่านระบบเสียงของ iPhone จะเป็นโปรแกรมสำคัญของ Apple โปรแกรมนี้มีความสามารถส่งข้อความ สร้างบันทึกจดจำ ค้นหาเว็บไซต์ และอื่น ๆ อีกมากมาย โดยใช้แค่เสียงสั่งการเท่านั้น ซึ่งจุดนี้เป็นการเริ่มต้นแนวใหม่ของอุปกรณ์ที่สั่งงานด้วยเสียง

๗. การสั่งงานผ่านท่าทาง ตอนนี้กำลังเป็นที่สนใจและนิยมอีกอย่างหนึ่งเช่นกัน จากอุปกรณ์เสริม XBOX 360 ที่ได้รับความนิยม Kinect จาก Microsoft อุปกรณ์ตัวนี้ สามารถควบคุมผ่านการขยับไปมาของมือในอากาศ ซึ่งอุปกรณ์ตัวนี้เป็นการจุดประกายให้สามารถใช้งานกับแพลตฟอร์มอื่นอีกด้วย

๘. หน้าจอแบบยืดหยุ่น เป็นนวัตกรรมใหม่ของจอ ที่ผู้ใช้สามารถซูมเข้า-ออก และเปลี่ยนหน้าหนังสือง่ายเพียงแค่บิดหมุนโทรศัพท์หรือแท็บเล็ต

โดยตอนนี้ Nokia และ Samsung เริ่มประกาศแล้วว่า บริษัทจะออกโทรศัพท์รุ่นใหม่ที่มีหน้าจอแบบนี้ในปี ๒๕๕๖

๙. HTML5 เป็นสิ่งที่จะทำให้นักพัฒนาแอปพลิเคชันสามารถสร้างสรรค์โปรแกรมที่สวยงามมากกว่าเดิม รวมไปถึงการตอบโต้กับผู้ใช้งานได้มากกว่าปัจจุบัน สาเหตุที่ควรจะมี HTML5 เนื่องมาจากว่านักพัฒนาพยายามสร้างแอปพลิเคชั่นสำหรับทุกระบบ OS จาก Android ไปหา iOS จากนั้นก็ไป Window Phone และอาจจะมีที่มากกว่านี้ในอนาคตมากไปกว่านั้น การที่ Adobe ออกมายกเลิกการสนับสนุนโปรแกรม Flash บนมือถือ เป็นสัญญาณบ่งชี้ว่าถึงการยกเลิกใช้งานบนมือถือและ HTML5 กำลังจะเข้ามาแทนที่

ภัยคุกคามด้านเทคโนโลยีสารสนเทศ

จากแนวโน้มและทิศทางเทคโนโลยีสารสนเทศในปี ค.ศ. ๒๐๑๓ ที่กล่าวข้างต้น นำไปสู่การวิเคราะห์และคาดการณ์ถึงภัยคุกคามด้านเทคโนโลยีสารสนเทศดังนี้

๑. ข้อผิดพลาดจากการกระทำของมนุษย์ ภัยคุกคามที่อันตรายที่สุดต่อความปลอดภัยของข้อมูลองค์กร คือ พนักงานขององค์กรเอง สิ่งที่พนักงานจะต้องปฏิบัติอย่างเคร่งครัดคือ การรักษาความลับของข้อมูล และข้อมูลพร้อมใช้งานได้ทุกเมื่อ

๒. การละเมิดทรัพย์สินทางปัญญา ทรัพย์สินทางปัญญาเป็นผลงานของผู้ที่เป็นเจ้าของความคิด ได้แก่ ลิขสิทธิ์เครื่องหมายการค้าและสิทธิบัตร คุณสมบัติของทรัพย์สินทางปัญญาอย่างหนึ่งคือ มีการระบุรหัสบ่งชี้ไว้อย่างเหมาะสม ส่วนใหญ่การละเมิดทรัพย์สินทางปัญญาจะเป็นการทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์

๓. การบุกรุก ทั้งในรูปแบบอิเล็กทรอนิกส์และกระทำโดยคนที่สามารถเข้าถึงข้อมูลที่เป็นความลับ เช่น การเข้าถึงข้อมูลด้วยการยืนข้างหลังมองข้ามไหล่ **(Shoulder Surfing)** เพื่อแอบดูหรือจำข้อมูลที่เป็นความลับ **Hacker** คือนักเจาะระบบที่มีความเชี่ยวชาญในการเขียนโปรแกรมเพื่อเข้าถึงข้อมูลที่มีการป้องกันอย่างผิดกฎหมาย **Cracker** คือการถอดรหัสหรือทำลายโปรแกรมที่ใช้ในการป้องกันการทำข้อมูลซ้ำเพื่อละเมิดลิขสิทธิ์

๔. การกรรโชกข้อมูลสารสนเทศ การขู่กรรโชกในการเปิดเผยข้อมูลที่เป็นความลับเกิดขึ้นจากการที่ข้อมูลที่เป็นความลับที่จัดเก็บอยู่ในระบบถูกขโมยไปอาจจะเป็นผู้บุกรุกจากภายนอกหรือผู้ที่มีหน้าที่ดูแลรักษาข้อมูลภายในองค์กร โดยมีการเรียกร้องค่าตอบแทนหรือค่าไถ่ (Ransom) แลกกับการที่จะไม่เปิดเผยข้อมูลความลับที่ได้ขโมยมา (Black Mail)

๕. การก่อวินาศกรรมหรือการทำลาย การกลั่นแกล้งทำลายทรัพย์สินก่อให้เกิดความเสียหายทำลายภาพพจน์ที่ดีขององค์กร ในบางครั้งการสร้างความเสียหายไม่จำเป็นต้องเป็นตัวเงินเสมอไป การโจมตีภาพพจน์ขององค์กรเช่นการทำลาย WebSite ส่งผลกระทบต่อความเชื่อมั่นขององค์กร

๖. การโจรกรรม การโจรกรรมทรัพย์สินทางกายภาพ เช่น เครื่องคอมพิวเตอร์ แนวทางการป้องกันคือการตรวจนับจำนวนสม่ำเสมอ Lock ประตูและติดตั้งระบบสัญญาณเตือนภัย ทรัพย์สินทางอิเล็กทรอนิกส์ต่างจากทรัพย์สินทางกายภาพ หากถูกขโมยไปตรวจพบได้ยากกว่า เนื่องจากนักโจรกรรมมีการปกปิดร่องรอย

๗. การโจมตีซอฟต์แวร์ การโจมตีซอฟต์แวร์เกิดขึ้นจากซอฟต์แวร์ที่ออกแบบให้โจมตีระบบเพื่อก่อความเสียหาย ทำลาย หรือปฏิเสธการบริการของ

ระบบของเป้าหมาย ซอฟต์แวร์ที่ได้รับความนิยมคือ Malicious Code หรือ Malicious Software มักจะเรียกว่า มัลแวร์ (Malware) มีมากมาย อาทิ ไวรัส (Viruses) เวิร์ม (Worms) ม้าโทรจัน (Trojan Horses) Logic bombs และประตูหลัง (Back doors)

๘. ภัยธรรมชาติ เป็นภัยคุกคามที่อันตรายมาก เพราะเป็นสิ่งที่เกินกว่ามนุษย์จะควบคุมได้ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ฟ้าผ่า ภูเขาไฟระเบิด ทั้งหมดนี้ไม่เพียงแต่สร้างความยุ่งยากต่อการใช้ชีวิตของแต่ละคนเท่านั้น แต่ยังสร้างปัญหาให้กับระบบคอมพิวเตอร์ทั้งหน่วยเก็บข้อมูล สัญญาณการสื่อสารต่าง ๆ

๙. คุณภาพของการบริการ ระบบสารสนเทศขององค์กรจะประสบความสำเร็จได้นั้นต้องได้รับการสนับสนุนจากระบบอื่น ๆ ร่วมด้วย เช่น โรงไฟฟ้า เครือข่ายโทรคมนาคม ผู้จัดจำหน่าย ผู้ให้บริการ ซึ่งระบบสนับสนุนเหล่านี้อาจหยุดชะงักได้หากเกิดพายุ พนักงานป่วย หรือเหตุฉุกเฉิน

๑๐. ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ ความล้มเหลวทางเทคนิคของฮาร์ดแวร์ หรือความผิดพลาดที่การผลิตอุปกรณ์เกิดข้อบกพร่องเป็นเหตุให้การทำงานของอุปกรณ์ภายนอกของระบบไม่เป็นไปอย่างที่คิด ส่งผลให้การบริการไม่น่าไว้วางใจ หรือใช้ประโยชน์ไม่ได้

๑๑. ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ การเขียนโค้ดคอมพิวเตอร์ส่วนมาก มีการตรวจสอบข้อผิดพลาดก่อนจำหน่าย ในบางครั้ง โปรแกรมเมอร์อาจสร้างชอร์ตคัตไว้ซึ่งอาจเป็นเหตุให้เกิดความเสียหายได้ เนื่องจากชอร์ตคัตสามารถเข้าสู่ตัวโปรแกรมได้โดยปราศจากการตรวจเช็คความปลอดภัยตั้งแต่เริ่มต้น

๑๒. เทคโนโลยีล้าสมัย โครงสร้างพื้นฐานที่ล้าสมัยทำให้ระบบไม่ปลอดภัย และไม่น่าไว้ใจ ผู้บริหารควรจะรู้ว่าเมื่อเทคโนโลยีล้าสมัย ส่งผลถึงความเสี่ยงด้านความมั่นคงของข้อมูล ควรมีการวางแผนรวมถึงการวิเคราะห์ในการเลือกใช้เทคโนโลยี เมื่อพบว่าเทคโนโลยีล้าสมัยต้องจัดการทันที

๑๓. ภัยจากไวรัสคอมพิวเตอร์ ปัจจุบันไวรัสคอมพิวเตอร์นิยมแพร่ผ่านอุปกรณ์เชื่อมต่อยูเอสบี เป็นการเปิดให้แฮ็กเกอร์เข้ามาทำลายข้อมูล นอกจากนี้ยังมี สปายแวร์ (Spyware) คือ โปรแกรมที่คอยสอดส่องการใช้งานเครื่องคอมพิวเตอร์ของเรา เกิดจากการเข้าชมเว็บไซต์ต่าง ๆ และดาวน์โหลดไฟล์ที่มีสปายแวร์ติดมาด้วย

๑๔. ภัยจากการขโมยข้อมูล ข้อมูลสำคัญทางคอมพิวเตอร์จะอยู่ในฮาร์ดดิสก์ ซึ่งมีวิธีนำออกมา ๒ แบบ คือ คนบุกเข้าไปขโมยจากเครื่องคอมพิวเตอร์และแฮ็กเกอร์ผ่านระบบ ประเภทแรก ส่วนใหญ่จะกระทำโดยพนักงานในองค์กรเพื่อปกปิดธุรกรรมที่ไม่ชอบ อีกประเภทใช้ช่องโหว่ของระบบลักลอบเข้าไปล้วงความลับ ทำลายข้อมูล เช่น การลบรายชื่อลูกหนี้การค้า

๑๕. ภัยจากการใช้อินเทอร์เน็ต เช่น การหลอกให้เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่าง ๆ อาทิ หมายเลขบัตรเครดิต ชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) โดยการส่งอีเมลเพื่อขอให้ “อัพเดต” หรือ “ยืนยัน” ข้อมูลบัญชี การหาเพื่อนคุยผ่านโปรแกรมสนทนา ทำให้เกิดการนัดหมายและล่อลวงไปทำมิดีมิร้าย สื่อลามกอนาจาร การเล่นเกมมากเกินไปจนไม่เข้าร่วมกิจกรรมกับสังคม

๑๖. ภัยจาก Web Application Hacking เป็นภัยจากแฮ็กเกอร์ที่เข้ามาเปลี่ยนหน้าเว็บไซต์ให้ไม่สามารถใช้งานได้ อย่างกรณีที่เคยเกิดขึ้นกับเว็บไซต์

ของกระทรวงไอซีที ไทยโพสต์ และไอเอ็นเอ็น เป็นต้น

๑๗. ภัยจาก Network infrastructure overloading กำลังเป็นภัยคุกคามรูปแบบใหม่ เกิดจากการดาวน์โหลดไฟล์คลิป ไฟล์ภาพยนตร์ จนทำให้อินเทอร์เน็ตช้าและระบบอาจล่มในที่สุด

๑๘. ภัยจากการละเลยคำเตือนของระบบการระวังภัย (Information Security) ขาดการวางแผนและการจัดระบบความปลอดภัยในคอมพิวเตอร์ดังนี้ การรักษาความปลอดภัยในคอมพิวเตอร์ส่วนบุคคล, การรักษาความปลอดภัยในระบบฐานข้อมูล, การรักษาความปลอดภัยในเครือข่ายการสื่อสารข้อมูล, การป้องกันทางกายภาพ, การวิเคราะห์ความเสี่ยง, ประเด็นในแง่กฎหมาย, จรรยาบรรณในเรื่องความปลอดภัยในระบบคอมพิวเตอร์ ตัวอย่างเช่นหากมีการสร้างการล็อกอินลวงระบบจะมีการแจ้งเตือน

จากการศึกษาแนวโน้มและทิศทาง ตลอดจนความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ พบว่าช่องโหว่และภัยคุกคามที่เกิดขึ้นในโลกของเทคโนโลยีสารสนเทศส่วนใหญ่เกิดขึ้นจากช่องโหว่ของการพัฒนาโปรแกรมประยุกต์ที่ไม่มั่นคงปลอดภัย (Insecure Application Development), การ Hack ข้อมูลผ่าน Wireless, การหลอกเอาข้อมูลส่วนตัว (Identity theft/Privacy Information Attack), การต้มตุ๋นหลอกหลวงในรูปแบบ Social Engineering และช่องโหว่ผ่านการใช้ประโยชน์โดยมิชอบจาก Social Network เช่น hi5, twitter, facebook, MySpace เป็นต้น สำหรับปี ค.ศ. ๒๐๑๓ กระแสของภัยคุกคามจะมาจากเว็บเซอร์วิส รวมถึงภัยการใช้ Social Network ดังนั้น ผู้ใช้งาน Social Network ที่ใส่ข้อมูลส่วนตัวมากเกินไปอาจตกเป็นเหยื่อของอาชญากรด้านเทคโนโลยีสารสนเทศได้ง่ายขึ้น โดยอาชญากรใช้หาข้อมูลส่วนตัวของเหยื่อโดยอาศัยข้อมูลจากเครือข่าย Social Network เป็นหลัก

สถิติการกระทำความผิดด้านเทคโนโลยีสารสนเทศ

จากข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ได้สรุปข้อมูลเกี่ยวกับเหตุภัยคุกคามที่ได้รับแจ้ง ซึ่งตรวจสอบและยืนยันว่าเกิดขึ้นจริงตั้งแต่เดือนมกราคมถึงเดือนธันวาคม พ.ศ. ๒๕๕๕ สรุปได้ดังนี้

๑. ประเภทภัยคุกคาม ใช้เกณฑ์ที่กำหนดโดย The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรป แบ่งเป็น ๙ ประเภท ได้แก่

๑.๑ เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) หมายถึง ภัยคุกคามที่เกิดจากการใช้หรือเผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน ข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (SPAM)

๑.๒ โปรแกรมไม่พึงประสงค์ (Malicious Code) หมายถึง ภัยคุกคามที่เกิดจากโปรแกรมที่ถูกพัฒนาขึ้นเพื่อให้เกิดผลที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) โดยปกติโปรแกรมประเภทนี้ผู้ใช้งานต้องเป็นผู้เปิดโปรแกรมก่อน จึงจะทำงานได้ เช่น Virus, Worm, Trojan, Spyware ต่าง ๆ

๑.๓ ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) หมายถึง ภัยคุกคามที่เกิดจากความพยายามรวบรวมข้อมูลจุดอ่อนของระบบ (Scanning) เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ

ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) การเก็บรวบรวมข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)

๑.๔ ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) หมายถึง ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)

๑.๕ การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) หมายถึง ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

๑.๖ การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) หมายถึง ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ อาจเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

๑.๗ การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) หมายถึง ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

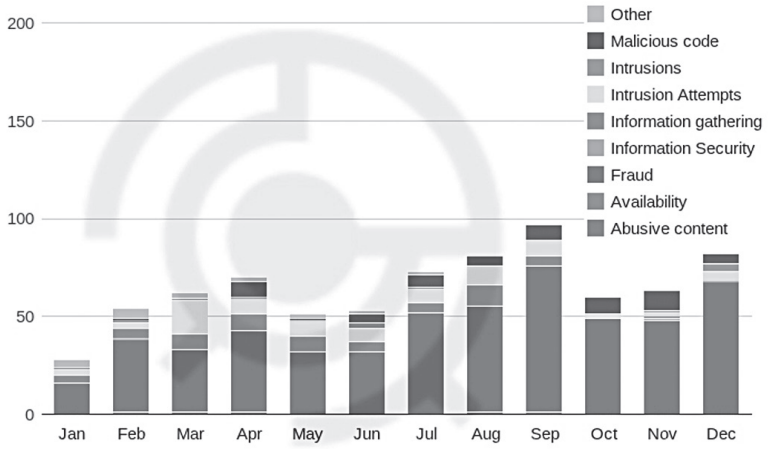
๑.๘ การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) หมายถึง ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต

๑.๙ ภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) หมายถึง ภัยคุกคามด้านเทคโนโลยีสารสนเทศประเภทอื่น ๆ นอกเหนือจากที่ได้กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น

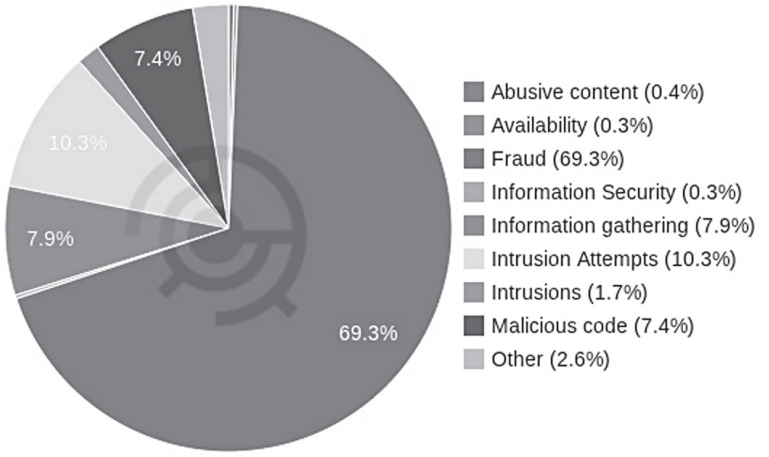
๒. สถิติภัยคุกคามในประเทศไทย เดือนมกราคม – ธันวาคม พ.ศ. ๒๕๕๕

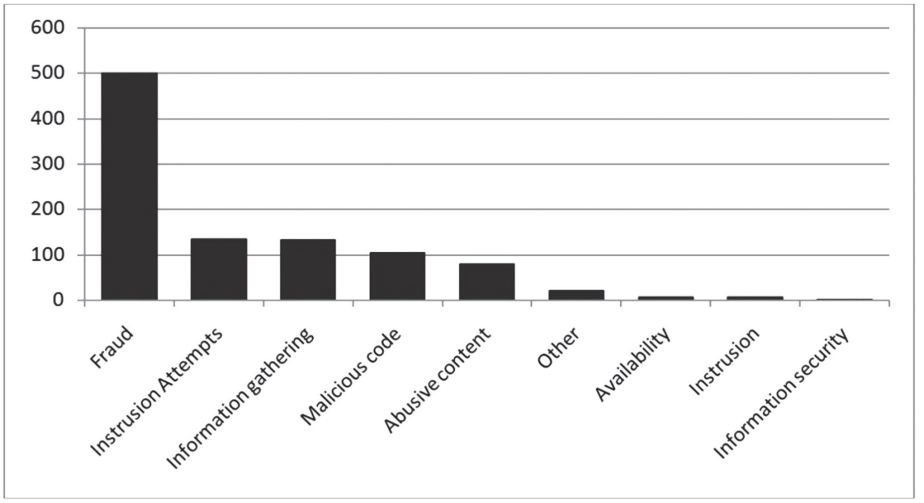
ประเภทภัยคุกคาม	พ.ศ.2555												รวม
	ม.ค.	ก.พ.	มี.ค.	เม.ย	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค	พ.ย.	ธ.ค.	
Abusive content	0	0	1	1	0	0	0	1	0	0	0	0	3
Availability	0	1	0	0	0	0	0	0	1	0	0	0	2
Fraud	16	37	32	42	32	32	51	54	74	49	48	67	534
Information gathering	4	5	10	8	8	5	5	10	5	0	1	1	62
Information security	0	1	0	0	0	0	0	0	0	0	1	0	2
Intrusion Attempts	3	3	13	8	8	6	7	10	8	2	2	5	75
Intrusion	1	1	1	1	0	3	1	0	0	0	1	4	13
Malicious code	3	6	9	12	7	4	7	3	8	8	10	5	82
Other	4	5	3	2	1	2	2	0	0	0	0	0	19
รวม	31	59	69	74	56	52	73	78	96	59	63	82	792

ภัยคุกคาม พ.ศ.2555 จำแนกรายเดือน



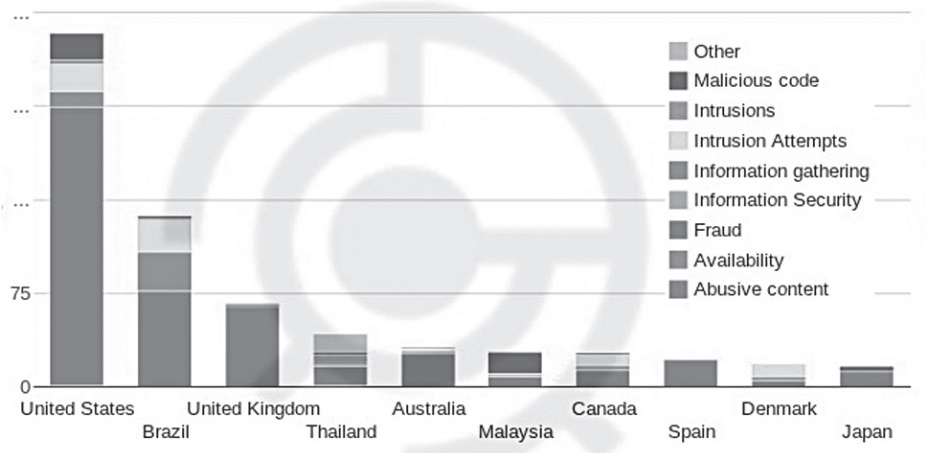
ภัยคุกคาม พ.ศ.2555 จำแนกรายประเภท





สถิติ ๑๐ อันดับประเทศที่แจ้งเหตุภัยคุกคามมากที่สุด พ.ศ. ๒๕๕๕

Country	Abusive Content	Availability	Fraud	Information security	Information Gatheri	Intrusion Attempt	Intrusio	Malicious Code	Other	Total
USA	1	0	223	0	13	22	3	21	0	283
Brazil	0	0	77	0	31	26	1	2	0	137
UK	0	0	64	0	1	0	0	1	1	67
Thailand	0	1	16	1	1	0	7	2	15	43
Australia	0	0	27	0	1	2	0	0	2	32
Malaysia	0	0	8	0	0	1	1	18	0	28
Canada	0	0	14	0	3	9	0	1	0	27
Spain	0	0	22	0	0	1	0	0	0	23
Denmark	0	0	5	0	3	11	0	0	0	19
Japan	0	0	12	1	0	0	0	4	0	17



สรุป

จากสถิติการแจ้งเหตุภัยคุกคามของประเทศไทย ตั้งแต่เดือนมกราคม – ธันวาคม พ.ศ. ๒๕๕๕ จะพบว่าการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) มีจำนวนสูงสุดคือ ๕๓๔ ครั้ง เมื่อเปรียบเทียบกับการเจาะระบบที่มีจำนวนต่ำกว่ามาก ซึ่งการเจาะระบบจะต้องทำโดยผู้ที่มีความรู้ความเชี่ยวชาญทางด้านเทคโนโลยีค่อนข้างสูง ส่วนการฉ้อฉลนั้นอาจใช้วิธีการหลอกลวง หรือเดาสุ่ม ซึ่งไม่ได้ใช้ความรู้ความสามารถทางด้านเทคโนโลยีมาก

จากสถิติการแจ้งเหตุภัยคุกคามของประเทศต่าง ๆ ปี พ.ศ. ๒๕๕๕ ประเทศไทยจัดอยู่ในอันดับที่ ๔ รองจากประเทศสหรัฐอเมริกา บราซิล และอังกฤษ ประเทศสหรัฐอเมริกามีพื้นที่ ๙,๖๒๙,๐๙๑ ตารางกิโลเมตร

มีประชากร ๓๑๒ ล้านคน เป็นประเทศที่มีขนาดใหญ่ มีประชากรมาก มีเทคโนโลยีที่ทันสมัย คนส่วนใหญ่เข้าถึงเทคโนโลยีสารสนเทศ จึงเป็นเหตุหนึ่งที่ทำให้มีการแจ้งเหตุภัยคุกคามสูงสุด ส่วนประเทศบราซิลก็เช่นกัน มีพื้นที่ ๘,๕๑๑,๙๖๕ ตารางกิโลเมตร มีประชากร ๑๘๙ ล้านคน มีขนาดใกล้เคียงกับประเทศสหรัฐอเมริกา มีประชากรมาก อาจเป็นเหตุให้มีการแจ้งภัยคุกคามสูงเช่นกัน ประเทศอังกฤษมีพื้นที่ ๒๔๔,๘๒๐ ตารางกิโลเมตร มีประชากร ๖๒ ล้านคน ใกล้เคียงกับประเทศไทย มีเทคโนโลยีสูง แต่ประเทศไทยมีพื้นที่ ๕๑๓,๑๑๕ ตารางกิโลเมตร มีขนาดเล็กกว่าประเทศสหรัฐอเมริกาถึง ๑๙ เท่า มีประชากร ๖๖ ล้านคน น้อยกว่าประเทศสหรัฐอเมริกา ๕ เท่า แต่ถูกจัดอันดับอยู่ที่ลำดับที่ ๔ เป็นประเทศขนาดเล็กแต่มีสถิติภัยคุกคามสูง สาเหตุเกิดจาก

๑. เป็นแหล่งที่อยู่ของเหล่าอาชญากรข้ามชาติ เนื่องจากเป็นประเทศเสรี นโยบายส่งเสริมการท่องเที่ยวทำให้มีต่างชาติเข้ามาอาศัยอยู่เป็นจำนวนมาก ยากต่อการตรวจสอบ และอาจส่งผลกระทบถึงนโยบายส่งเสริมการท่องเที่ยว

๒. กฎหมายไม่มีประสิทธิภาพ ไม่ครอบคลุมรูปแบบการกระทำความผิดเกี่ยวกับเทคโนโลยีสารสนเทศ มาตรการบังคับใช้กฎหมายที่ยังไม่เข้มงวดและจริงจัง

๓. หน่วยงานที่เกี่ยวข้องยังไม่พร้อม ไม่มีอำนาจเพียงพอเนื่องจากเป็นหน่วยที่ทำหน้าที่ประสานงาน มีจำนวนบุคลากรไม่เพียงพอ บุคลากรยังมีความรู้ความเชี่ยวชาญน้อย ขาดเครื่องมือและงบประมาณในการดำเนินงาน เมื่อพบการกระทำความผิดต้องแจ้งเจ้าหน้าที่ตำรวจเพื่อดำเนินการ

การแจ้งเหตุภัยคุกคามพบว่าส่วนใหญ่เป็นเรื่องภัยที่เกิดจากการกระทำของมนุษย์ เกิดจากความต้องการให้ได้มาซึ่งข้อมูลอันเป็นประโยชน์ต่อตัวเองโดยมิชอบ พยายามเข้าถึงระบบ หรือข้อมูลที่ตนเองไม่มีสิทธิ์ เป็นการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ การป้องกันกระทำได้หลายวิธีทั้งการติดตั้งระบบป้องกัน การควบคุมการเข้าถึงข้อมูล การตรวจสอบการทำงานตามขั้นตอนของการรักษาความปลอดภัยขององค์กร แต่สิ่งที่สำคัญที่สุดก็คือบุคลากรขององค์กรต้องตระหนักถึงความสำคัญของมาตรการรักษาความปลอดภัยอย่างเคร่งครัด

ข้อเสนอแนะ

จากสถิติที่ประเทศไทยมีการแจ้งเหตุภัยคุกคามสูงเป็นอันดับที่ ๓ ของโลก และสาเหตุดังกล่าวข้างต้น ควรมีการปรับปรุงพัฒนาในเรื่องดังต่อไปนี้

๑. ปรับปรุงและพัฒนากฎหมายที่เกี่ยวข้อง ให้มีความทันสมัยครอบคลุมรูปแบบภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา โดยกำหนดหน่วยงาน.....(ที่รับผิดชอบ)

๒. ปรับโครงสร้างหน่วยงานที่เกี่ยวข้อง ให้มีประสิทธิภาพ เพิ่มอำนาจ ตลอดจนบุคลากรและงบประมาณให้เพียงพอที่จะปฏิบัติงานได้อย่างมีประสิทธิภาพ

๓. เพิ่มมาตรการในการตรวจสอบ ติดตามพฤติกรรมของบุคคลต้องสงสัยว่าจะเป็นภัยคุกคามด้านเทคโนโลยีสารสนเทศ

๔. ส่งเสริมและสนับสนุนหน่วยงานองค์กรต่าง ๆ ทั้งภาครัฐและเอกชนให้มีการจัดทำมาตรการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างจริงจัง ให้เป็นไปตามมาตรฐานสากล

๕. ส่งเสริมรวมทั้งปลูกฝังเยาวชนรุ่นใหม่ ที่กำลังก้าวสู่ยุคดิจิทัลให้มีจิตสำนึกในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้รู้ถึงภัยคุกคาม ผลเสียหายอันเกิดจากการไม่รักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

การรักษาความมั่นคงปลอดภัยข้อมูลในระบบสารสนเทศจำเป็นต้องมีการศึกษาเรียนรู้และติดตามสถานการณ์ความเปลี่ยนแปลงทั้งด้านเทคโนโลยีและภัยคุกคามที่มีการเปลี่ยนแปลงอย่างรวดเร็ว เพื่อให้รู้เท่าทันและนำมาปรับปรุงพัฒนามาตรการรักษาความมั่นคงปลอดภัยขององค์กรให้มีประสิทธิภาพสูงสุดและที่สำคัญที่สุดคือการให้ความรู้และการสร้างความตระหนักถึงภาระหน้าที่และความรับผิดชอบในการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่องค์กรกำหนดขึ้น

แหล่งข้อมูล

๑. นิพนธ์ นาธิน, ผู้จัดการอาวุโสแผนกที่ปรึกษาด้านเทคนิค บริษัท เอซิส โปรเฟสชั่นนั่ล เซ็นเตอร์ จำกัด. บรรยายเรื่อง “แนวโน้มภัยคุกคามความปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ ในปี ค.ศ. ๒๐๑๒-๒๐๑๓”. ณ ศูนย์เทคโนโลยีสารสนเทศ, ๒๗ มีนาคม ๒๕๕๕

๒. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. “ประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดย eCSIRT”. (ออนไลน์). เข้าถึงได้จาก : //http:www.thaicert.or.th/papers/normal/2012/pp2012no0001.html ๒๕๕๕

๓. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. “สถิติภัยคุกคาม พ.ศ. ๒๕๕๕”. (ออนไลน์). เข้าถึงได้จาก : http://www.thaicert.or.th/statistics/statistics.html

๔. เศรษฐพงค์ มะลิสุวรรณ. “ภัยคุกคามความมั่นคงระบบสารสนเทศ”. วิทยานิพนธ์, มหาวิทยาลัยกรุงเทพ, ๒๕๕๒

๕. อนุดิษฐ์ นาครทรรพ, รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. บรรยายเรื่อง “การพัฒนานโยบายความมั่นคงแห่งชาติของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร”. ณ วิทยาลัยป้องกันราชอาณาจักร, ๑๘ กรกฎาคม ๒๕๕๕

๖. JulietSoft. “แนวโน้มเทคโนโลยี ปี พ.ศ. ๒๕๕๖ (ค.ศ. ๒๐๑๓) โดยการ์ดเนอร์”. (ออนไลน์). เข้าถึงได้จาก : http://202.52.6.183/jssoft/wp-content/uploads/2013/01/trend_Dr.Prasong_OK.pdf