รายงานข่าววิทยาศาสตร์และเทคโนโลยี จาก

วอชิงตัน

สำนักงานที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยี ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน

เดือนธันวาคม 2560
ฉบับที่ 12/2560

Cyber Security
ความปลอดภัยไซเบอร์
ปัญหาความมั่นคงของสังคมยุคใหม่

รายงานข่าววิทยาศาสตร์และเทคโนโลยีจากวอชิงตัน
ฉบับที่ 12/2560 ประจำเดือนธันวาคม 2560

บรรณาธิการที่ปรึกษา:
ดร.เศรษฐพันธ์ กระจ่างวงษ์
ผู้ช่วยทูตฝ่ายวิทยาศาสตร์และเทคโนโลยี

กองบรรณาธิการ:
นางสาวบุณยเกียรติ รักษาแพ่ง
นางสาวดวงกมล เพิ่มพูลทวีทรัพย์
นายอิศรา ปทุมานนท์

จัดทำโดย
สำนักงานที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยี
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน ดี.ซี.
1024 Wisconsin Ave., N.W. Suite 104
Washington, D.C. 20007
โทรศัพท์: +1 (202)-944-5200
Email: ost@thaiembdc.org

ติดต่อคณะผู้จัดทำได้ที่
Website: http://www.ost.thaiembdc.org
Email: ost@thaiembdc.org
Facebook: https://www.facebook.com/ostsci/

สารบัญ

สวัสดีท่านผู้อ่านที่เคารพรักทุกท่าน

และแล้ว วันนี้ เราก็มาถึงรายงานข่าววิทยาศาสตร์และเทคโนโลยีจากวอชิงตันฉบับสุดท้ายของปี 2560 แล้วนะครับ สำหรับฉบับเดือนธันวาคม 2560 ส่งท้ายปีเก่านี้ ทางทีมงานฯ ได้นำเสนอ เรื่องน่าสนใจด้านวิทยาศาสตร์และเทคโนโลยี ที่ได้รับความสนใจในสังคมอเมริกัน ซึ่งเป็นประเทศที่มีการใช้เครือข่ายโทรคมมาคมทั้งมีสาย ไร้สาย มากที่สุดในโลก และเป็นประเทศต้นแบบการพัฒนาการสื่อสารโทรคมนาคมแบบเสรีมานำเสนอท่านผู้อ่าน นั่นก็คือเรื่องความปลอดภัยบนโลกออนไลน์ (Cyber Security) ซึ่งเป็นประเด็นความมั่นคง ที่รัฐบาลสหรัฐให้ความสนใจอย่างมาก และพยายามมีการบัญญัติและบังคับใช้กฎหมาย และคิดค้นเทคโนโลยีใหม่ๆ มาจัดการกับภัยคุกคามบนโลกออนไลน์ที่ไร้พรมแดนนี้ ที่ยังมีอาชญากรและเชื้อโรคตัวใหม่เข้ามาบ่อนทำลายอยู่เสมอๆ

รายงานฉบับนี้ จะได้นำเสนอปัญหาและแนวทางแก้ไขปัญหาต่างๆ ของภาครัฐและเอกชนของสหรัฐที่เกี่ยวข้องกับโลกออนไลน์ หรือ ระบบอินเทอร์เน็ต รวมทั้ง ยังได้เสนอแง่มุมเปรียบเทียบกับนโยบายด้านไซเบอร์ของสาธารณรัฐประชาชนจีน ยักษ์ใหญ่ธุรกรรมออนไลน์แห่งโลกตะวันออกด้วย และที่พลาดไม่ได้อย่าลืมอ่านบทวิเคราะห์ ภาพยนตร์ SCI FI กับความหมาย วนท. นะครับ รอบนี้ แม้ภาพยนตร์จะไม่ใช่ฟอร์มยักษ์ แต่ก็สะท้อนความเป็นจริงของการมาเงียบๆ ของมหันตภัยทางไซเบอร์ (ตามสไตล์เพลงของแก้ม วิชญาณี) ได้เป็นอย่างดี

ในศุภวาระดิถีขึ้นปีใหม่ 2561 นี้ ทีมงานขออาราธนาสิ่งศักดิ์สิทธิ์ทั้งหลายในสากลโลก โปรดดลบันดาลให้ท่านทั้งหลาย มีความสุข สุขภาพแข็ง มีพลังและสติปัญญาที่จะนำพาตนเอง ครอบครัว สังคม ก้าวหน้า เจริญรุ่งเรือง และนำพาประเทศไทยของเราไปสู่ยุคไทยแลนด์ 4.0 ด้วยเทอญ

ทีมบรรณาธิการ
สำนักงานที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยี
ประจำสถานเอกอัครราชทูต ณ กรุงวอชิงตัน

แผนปฏิบัติการความมั่นคงทาง CYBER ในสหรัฐอเมริกา

สหรัฐอเมริกา ถือว่า เป็นประเทศชั้นนำและประเทศต้นแบบ ในการนำสังคมโลกไปสู่สังคมของการสื่อสารโทรคมนาคมแบบไร้พรมแดน โดยเฉพาะการเป็นประเทศที่มีนโยบายเปิดกว้างทางการสื่อสาร ยิ่งทำให้พัฒนาการด้านเทคโนโลยีสื่อสารโทรคมนาคม และสารสนเทศ เป็นไปอย่างรวดเร็ว บนเบื้องหน้าของความรุ่งโรจน์ของการสื่อสารทางอิเล็กทรอนิกส์ ที่ช่วยสนับความคล่องตัวในการประกอบธุรกรรม และการติดต่อสื่อสาร ก็ปรากฏเบื้องหลังในมุมมืดที่เทคโนโลยี นี้ถูกใช้ไปในทางอกุศล ตั้งแต่ระดับการแข่งขันต่อสู้กับคู่ธุรกิจ ไปจนถึงเงื่อนงำที่เกี่ยวข้องอบายมุข อาชญากรรมทางไซเบอร์ ไปจนถึงการก่อการร้ายข้ามชาติ

กฎระเบียบด้านความปลอดภัยทางอินเทอร์เน็ต หรือ cyber security จึงเป็นประเด็นร้อนอย่างหนึ่งที่ทั่วโลก โดยเฉพาะรัฐบาลสหรัฐจับตามองเมื่อสินทรัพย์และเงินทอง ทั้งที่จับต้องได้ เช่นสินค้า และจับต้องไม่ได้ เช่นข้อมูลสำคัญ สามารถถูกยักยอกหรือทำลาย ได้ด้วยกระบวนการทางเทคโนโลยีการสื่อสาร การโจมตีทาง Cyber หรือ cyber attack มีมานาน และมีกลไกที่หลากหลาย เทียบเคียงได้กับการติดเชื้อร่างกายของมนุษย์ ไม่ว่าจะเป็น virus, worms, Trojan horses, phising denial of service (DOS) attack unauthorized access เป็นต้น

สหรัฐฯ เป็นประเทศที่มีมาตรการ ในการรักษาความปลอดภัยประกอบด้วย Firewalls, antivirus software การตรวจจับการรุกราน (intrusion detection) และระบบป้องกันอื่นๆ มากที่สุดและก็เป็นประเทศที่มีการใช้ระบบสื่อสารอินเทอร์เน็ต ไปในทางที่ไม่เหมาะสมมากที่สุด รวมถึงการทำร้ายช่วงชิง หน่วงเหนี่ยว กักกัน หรือสังหารระบบคอมพิวเตอร์ของศัตรู หรือเหยื่อ ดังนั้น จึงเป็นประเทศที่มีความก้าวหน้าในการพัฒนาด้านเทคโนโลยี และกฎหมายทาง Cyber security ที่มีความชัดเจนมากที่สุดในโลกเช่นกัน

กฎระเบียบแรกๆ ของสหรัฐฯ ในด้าน cyber security ที่มีอยู่ คือ Health Insurance Portability and Accountability Act (HIPAA) ค.ศ. 1999 Gramm–Leach–Bliley Act ค.ศ. 2002 และ Homeland Security Act ค.ศ. 2002 ซึ่งรวมถึง Federal Information Security Management Act (FISMA) กฎระเบียบ 3 ชุดนี้ ช่วยให้องค์ที่มีภารกิจที่ล่อแหลม

แผนปฏิบัติการความมั่นคงทาง CYBER ในสหรัฐอเมริกา

ต่อการถูกโจมตี ได้แก่ บรรษัทประกัน สถาบันการเงิน และหน่วยงานราชการ ต้องพัฒนาระบบป้องกันของตนเอง ตัวอย่างเช่น FISMA ซึ่งใช้กับหน่วยงานราชการทั่วไป ต้องมีการพัฒนาและใช้งานระบบความปลอดภัย ตามนโยบาย หลักเกณฑ์ มาตรฐาน และแนวทาง ที่วางไว้โดยกฎนี้ อย่างไรก็ตาม กฎหมายเหล่านี้ ไม่ได้บังคับใช้ครอบคลุมกับผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers) และบริษัทซอฟต์แวร์ การพัฒนาเทคโนโลยีสารสนเทศด้านนวัตกรรม ก็ยังคงถูกการพัฒนาเทคโนโลยีด้านจารกรรมหาช่องโหว่อยู่ บางมลรัฐได้ตั้งกฎระเบียบของตนเอง อาทิ มลรัฐแคลิฟอร์เนียร์ ซึ่งมีกฎหมายเคร่งครัด เกี่ยวกับการควบคุมการรั่วไหลของข้อมูลบุคคล Notice of Security Breach Act เป็นต้น

ความก้าวหน้าใน ด้านมาตรการทางกฎหมายที่สำคัญของสหรัฐได้มีขึ้นในชื่อของ Cyber Security Act 2015 ที่ได้มีการวางแนวทางและมาตรการที่เรียกว่า Cybersecurity National Action Plan (CNAP) ไว้อย่างครอบคลุม ไม่ว่า จะเป็นการสร้างความตระหนัก การคุ้มครองข้อมูลปัจเจกบุคคล และความปลอดภัยทางสังคม โดยมีการตั้งคณะกรรมการที่ชื่อว่า Commission on Enhancing National Cybersecurity ที่เป็นที่รวมของสุดยอดนักคิดในด้านยุทธศาสตร์ ด้านธุรกิจ และด้านเทคนิคไว้ด้วยกัน ดังนั้น จึงเป็นคณะกรรมการที่คิดค้นทั้งกฎหมายระเบียบ วิธีประกอบธุรกิจที่ปลอดภัย รวมทั้งการพัฒนาเทคนิคซอฟต์แวร์ต่างๆ ไว้ด้วยกันอย่างเป็นบูรณาการ

แต่ก็ที่แน่นอน พระเอกจะดูดีได้ ผู้ร้ายต้องเหี้ยมโหด อาชญากรไซเบอร์ชั้นนำของโลกก็ดำเนินกิจกรรมท้าทายกฎหมายอยู่อย่างต่อเนื่องแม้กระทั่งหลังจากได้มีการประกาศใช้ พรบ. นี้ ที่มีการระดมกองทุนรองรับที่ชื่อว่า Information Technology Modernization Fund กว่า 3100 ล้านดอลลาร์สหรัฐ เพื่อพัฒนาปรับปรุงระบบอินเทอร์เน็ตของทั้งภาครัฐบาลและเอกชนที่มีความเสี่ยง ภายใต้การบริหารจัดการของ Federal Chief Information Security Officer

กลไกหนึ่งที่เป็นทางเลือกสำคัญในการเพิ่มความปลอดภัยให้กับโลกอินเทอร์เน็ต คือ การใช้การตรวจสอบข้อมูลส่วนตัวแบบซับซ้อน หรือ multi-factor authentication ซึ่งเป็นมาตราการทั้งแบบเทคโนโลยี และการตรวจสอบโดยการซักถามจากผู้ให้บริการ กล่าวง่ายๆ คือให้นอกจากจะพัฒนาระบบแล้ว ก็ให้ประชาชนมีสำนึกถึงความปลอดภัยในการยอมให้มีตรวบสอบข้อมูล โดยการถามการกรอก ให้มากขึ้น โดยไม่เคืองผู้ให้บริการ โดยระบบนี้ ได้มีการสร้างเครือข่ายพันธมิตรร่วมปฏิบัติการ (National Cyber Security Alliance) ซึ่งพันธมิตรเหล่านี้ เราก็จะคุ้นชื่อกันดี เช่น Google Facebook Dropbox และ Microsoft รวมทั้งบริษัทที่ให้บริการทางการเงินเช่น MasterCard, Visa, Paypal, และ Venmo ที่ลดระบบรูดปื๊ดๆ แบบเสรีลงไป (ซึ่งต่างจากระบบของจีน ที่การใช้บัตรเครดิตทุกครั้งต้องมีการกดรหัส Pin Number 6 หลัก) มาตั้งแต่เริ่มต้นแล้ว

แผนปฏิบัติการความมั่นคงทาง CYBER ในสหรัฐอเมริกา

ในปี 2560 นี้ งบประมาณกว่า 19,000 ล้านดอลล่าร์ของสหรัฐ จึงได้ถูกระดมมาเพื่อกิจการด้านความปลอดภัยทาง Cyber เพิ่มเติม เนื่องจากความรุนแรงของอาชญากรรมทางไซบอร์ไม่ได้ลดลง และกระแสข่าวของภัยดังกล่าว ยังคงเกิดขึ้นอย่างต่อเนื่อง เช่น การล้วงข้อมูลของ Yahoo และ Equifax ที่เป็นข่าวโด่งดังในปี 2560 หรือ การแพร่ระบาดของไวรัส wannacry ที่โดนเข้า ก็ต้องร้องกรี๊ดตามชื่อของมัน ซึ่งจริงๆ แล้ว ก็ไม่เป็นเรื่องที่น่าแปลก เนื่องจากการดำเนินธุรกรรมออนไลน์ ได้ขยายตัวเพิ่มมากขึ้นเรื่อยๆ ในปัจจุบัน พร้อมกับในอินเทอร์เน็ตเองก็มีคำแนะนำในการก่ออาชญากรรมที่ยังพอหาได้จากบางเว็บไซต์ โดยยังไม่มีหน่วยงานใดเข้ามาจัดการ เช่น ใน listverse.com ได้เสนอบทความ Top 10 tips to commit perfect crime ซึ่งบรรยายแนวทางก่ออาชญากรรมไว้อย่างน่าฉงน

คำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) จึงเป็นคำที่มีความหมายใหญ่โตในโลกปัจจุบัน ภัยหลายๆ อย่างต้องอาศัยช่องทางเข้าถึงตัวผ่านประตูหน้าต่าง แต่ภัยทางไซเบอร์นั้น ขอเพียงคุณมีมือถือติดตัว หรือคอมพิวเตอร์ติดตัว มันอาจมาจู่โจมคุณโดยไม่รู้ตัวได้ทุกเวลาที่คุณเพลิดเพลินกับอุปกรณ์สื่อสารที่รับส่งสัญญาณได้ของคุณเอง

การจู่โจมทางไซเบอร์ที่ส่งผลกระทบกับคนจำนวนมาก

การโจมตีทางไซเบอร์มีหลากหลายรูปแบบโดยเฉพาะในสหรัฐอเมริกาซึ่งมีระบบเครือข่ายการให้บริการอินเตอร์เน็ตที่ใหญ่ที่สุดของโลก หลายๆ ครั้งเหตุการณ์ก็เกิดขึ้นโดยที่สาธารณะไม่เคยรับรู้ แต่หลายๆ เหตุการณ์ก็เป็นข่าวใหญ่เพราะการโจมตีส่งผลกระทบกับคนจำนวนมากๆ เหตุการณ์โจมตีดังต่อไปนี้ เป็นการโจมตีไซเบอร์ที่ก่อความเดือดร้อนต่อความมั่นคงและกิจกรรมทางเศรษฐกิจ รวมถึง ส่งผลกระทบต่อระบบฐานข้อมูลส่วนตัวธุรกรรมของปัจเจกชน และนี่คือตัวอย่างเหตุการณ์ในปี 2560 ที่เป็นข่าวใหญ่ในสังคมอเมริกันและทั่วโลก

① ไวรัส WannaCry

ในวันที่ 12 พฤษภาคม พ.ศ. 2560 ไวรัสเรียกค่าไถ่ Wannacry ได้แพร่กระจายและเข้าถึงคอมพิวเตอร์กว่าแสนเครื่องทั่วโลก ซึ่งแม้แต่ระบบคอมพิวเตอร์ขององค์กรขนาดใหญ่ก็ตกเป็นเหยื่อ เช่น การโจมตีนี้ทำให้โรงพยาบาลหลายแห่งในสหราชอาณาจักรไม่สามารถใช้ระบบคอมพิวเตอร์ได้ ส่งผลเสียหายกับผู้ป่วยจำนวนมาก หน่วยงานข่าวกรองของสหรัฐ–อเมริกาได้ออกมาประกาศด้วยความมั่นใจ “ระดับกลาง” ว่าไวรัสตัวนี้เป็นผลงานของรัฐบาลเกาหลีเหนือ

2. การจู่โจมบริษัทข้อมูลเครดิต

บริษัทข้อมูลเครดิต Equifax ของสหรัฐฯ ซึ่งเป็นบริษัทที่มีระบบฐานข้อมูลเครดิตบุคคลที่ใหญ่ที่สุดได้ออกมาประกาศเมื่อเดือนกรกฎาคม พ.ศ. 2560 ว่าเว็บไซต์ของบริษัทถูกอาชญากรไซเบอร์จู่โจมและดึงเอาข้อมูลส่วนบุคคลของลูกค้ากว่า 150 ล้านคน การถูกโจมตีครั้งนี้ ถือว่าเป็นความผิดพลาดครั้งใหญ่ของ Equifax เพราะ บริษัทได้เตรียมการที่จะเปลี่ยนแปลงระบบป้องกันและรูปแบบวิศวกรรมของระบบคอมพิวเตอร์เพื่อเตรียมรับมือกับการโจมตีไซเบอร์แล้ว แต่จากกระบวนการที่ล่าช้าทำให้ระบบฐานข้อมูลถูกโจมตีไปเสียก่อน

3.การรั่วไหลของข้อมูลผู้ใช้บริการเว็บไซต์ Yahoo

เว็บไซต์ Yahoo เป็นบริษัทที่มีผู้ใช้บริการทั่วโลกโดยเฉพาะ Yahoo Email บริษัทได้เพิ่งออกมายอมรับเมื่อเดือนตุลาคม พ.ศ. 2560 ว่า ในปี พ.ศ. 2557 อาชญากรไซเบอร์ได้ขโมยเอาข้อมูล Yahoo Email กว่า 3 ล้านชื่อไปได้ โดยข้อมูลที่ได้ไป อาชญากรสามารถเข้าไปดูข้อมูลในอีเมล์ได้ทั้งหมด ผู้เชี่ยวชาญเชื่อว่าบริษัท Yahoo จงใจเก็บเรื่องนี้เป็นความลับ เนื่องจาก บริษัทกำลังจะขายกิจการให้กับบริษัท Verizon ซึ่งเป็นบริษัทผู้ให้บริการอินเตอร์เน็ตยักษ์ใหญ่เจ้าหนึ่งของสหรัฐฯ เหตุการณ์นี้ทำให้หลายๆ คนรู้สึกหวาดกลัวในความปลอดภัยในโลกไซเบอร์ เพราะการกระทำของบริษัท Yahoo แสดงให้เห็นว่าบริษัทไม่ได้สนใจผลที่จะตามมาที่จะกระทบต่อผู้ใช้บริการ Yahoo Email จำนวนมาก เพียงเพราะต้องการปกป้องผลประโยชน์ของบริษัทเอง และเชื่อว่ายังมีอีกหลายเหตุการณ์ที่ยังถูกปิดเป็นความลับจากประชาชนทั่วไป

④. การรั่วไหลของข้อมูลลูกค้าที่ใหญ่ที่สุดของบริษัทค้าปลีก Target

บริษัทค้าปลีก Target ถูกอาชญากรไซเบอร์ใช้จุดอ่อนในระบบคอมพิวเตอร์ของบริษัท เข้าไปขโมยข้อมูลบัตรเครดิต ชื่อจริง ข้อมูลการติดต่อต่างๆ ของลูกค้ากว่า 41 ล้านราย และเฉพาะข้อมูลการติดต่อของลูกค้าอีก 60 ล้านรายในเดือนพฤศจิกายน พ.ศ. 2557 มลรัฐของสหรัฐฯ จำนวน 41 มลรัฐและกรุงวอชิงตัน ได้ดำเนินคดีกับบริษัท Target และในที่สุดบริษัทยอมจ่าย 18.5 ล้านเหรียญสหรัฐฯ ให้แก่มลรัฐต่างๆ เพื่อระงับข้อพิพาท ซึ่งเงินจำนวนนี้ก็จะถูกนำไปใช้ในการให้ข้อมูลและแก้ไขปัญหาที่เกิดจากการรั่วไหลของข้อมูลให้แก่ลูกค้าต่อไป

5. บริษัท Uber ยอมจ่ายค่าไถ่ให้แฮกเกอร์เพื่อปกป้องข้อมูล

ในปี พ.ศ. 2559 บริษัท Uber ถูกขโมยข้อมูลของลูกค้าและคนขับรถกว่า 57 ล้านราย บริษัทไม่ได้ดำเนินคดีกับอาชญากรรายนี้ แต่ยอมจ่ายค่าไถ่ให้กับแฮกเกอร์เป็นเงินจำนวน 1 แสนเหรียญฯ แม้ว่าบริษัทจะยังไม่ทราบว่าแฮกเกอร์กลุ่มนี้คือใคร หลังจากที่บริษัทได้ตกลงกับแฮกเกอร์แล้ว บริษัทได้ปรับปรุงระบบความปลอดภัยไซเบอร์ให้ดีขึ้น

ที่มา: https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html
https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/
https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers/

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

ปี พ.ศ. 2561 จะเป็นอีกปีที่ปัญหาด้านความปลอดภัยไซเบอร์ยังเป็นความท้าทายที่ทั่วโลกต้องเผชิญ ผู้เชี่ยวชาญได้คาดการณ์ไว้ว่าความเคลื่อนไหวด้านความปลอดภัยไซเบอร์ในปีหน้านี้จะมีผลกระทบต่อหลากหลายวงการ ไม่ว่าจะเป็นความปลอดภัยของรัฐบาลของสหรัฐอเมริกาฯ การรับมือกับปัญหาข่าวปลอม การบังคับใช้ GDPR (General Data Protection Regulation ซึ่งเป็นร่างกฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคฉบับใหม่ของ EU) และการพัฒนาเทคโนโลยีใหม่ต่างๆ เช่น Internet of Things (IoT) และ Artificial Intelligence (AI) ค่าเงินดิจิตอล (cryptocurrency) และ ไบโอแมทริกซ์ (biometrics หรือการใช้ข้อมูลทางชีวภาพ) และรวมไปถึงปัญหาความขาดแคลนแรงงานที่มีทักษะด้านความปลอดภัยทางไซเบอร์ โดยมีรายละเอียดดังนี้

การโจมตีรัฐบาลและโครงสร้างพื้นฐานที่สำคัญของสหรัฐอเมริกา

– หน่วยงานข่าวกรองสหรัฐฯ รายงานว่า เนื่องจากความขัดแย้งระหว่างสหรัฐอเมริกาและเกาหลีเหนือทวีความรุนแรงมากยิ่งขึ้น เกาหลีเหนือซึ่งได้รับการสนับสนุนจากประเทศรัสเซียและประเทศจีนจะเริ่มการโจมตีทางไซเบอร์ที่รุนแรงขึ้นโดยยึดรูปแบบและกลยุทธ์จากประเทศรัสเซีย เช่น การเขียนข่าว และรายงานปลอมเพื่อบั่นทอนความมั่นคง และสร้างความขัดแย้ง ในสหรัฐอเมริกา ฯลฯ

– ในช่วงสองปีที่ผ่านมา สหภาพยุโรปได้ตกเป็นเหยื่อของการโจมตีไซเบอร์ที่มุ่งไปที่เครือข่ายเชื่อมโยงระบบไฟฟ้า (power grid) และโรงงานผลิตต่างๆ ในปีหน้านี้ เป้าหมายจะเปลี่ยนมาเป็นสหรัฐ–อเมริกา หน่วยงาน FBI และ United States Department of Homeland Security (DHS) ได้เตือนให้หน่วยงานต่างๆ ระวังการโจมตีทางไซเบอร์โดยเฉพาะในส่วนที่เกี่ยวข้องกับพลังงาน เทคโนโลยีนิวเคลียร์ น้ำประปา การบิน การก่อสร้าง และการผลิตต่างๆ

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

การขโมยข้อมูลส่วนบุคคลและการบังคับใช้ GDPR

- ความพยายามในการขโมยข้อมูลส่วนบุคคลเช่น ข้อมูลทางการแพทย์ ข้อมูลของรัฐบาล และข้อมูลทางการเงินซึ่งมีให้เห็นแล้วในช่วง 2 – 3 ปีที่ผ่านมา ในปีหน้าที่จะทวีความรุนแรงมากยิ่งขึ้น
- ข้อมูลประจำตัว (Personally Identifiable Information – PII) ต่างๆ จะไม่เป็นความลับส่วนบุคคลอีกต่อไป ซึ่งเป็นผลมาจากการรั่วไหลของข้อมูลจากช่องทางต่างๆ ที่เกิดขึ้นอย่างต่อเนื่องระหว่าง 2 – 3 ปีที่ผ่านมา ในปีหน้านี้อาชญากรจะรวบรวมและใช้ข้อมูลส่วนบุคคลที่รั่วไหลเหล่านี้ในการโจมตีทางไซเบอร์โดยใช้ระบบสังคมเป็นเครื่องมือ (social engineering attacks หรือ การโจมตีที่ใช้การปฏิสัมพันธ์ของมนุษย์เป็นเครื่องมือในการทำลายมาตรการรักษาความปลอดภัย)

- ในปี พ.ศ. 2561 จะมีการบังคับใช้กฎหมายและข้อบังคับต่างๆ ของ GDPR มากยิ่งขึ้น โดยสภาพยุโรปจะเป็นตัวตั้งตัวตีในการเตรียมความพร้อมเพื่อป้องกันข้อมูลส่วนบุคคลในระดับโลก และเราจะได้เห็นประเทศต่างๆ ทั่วโลกให้ความร่วมมือกับสหภาพยุโรปมากยิ่งขึ้น
- ข้อมูลจากการจองหรือชำระค่าตั๋วเดินทางต่างๆ จะเป็นช่องทางสำคัญที่อาชญากรไซเบอร์ใช้ในการเข้าถึงข้อมูลที่เกี่ยวกับพาสปอร์ต หมายเลขบัตรเครดิต บ้านเลขที่ ข้อมูลการติดต่อต่างๆ หรือแม้แต่ข้อมูลเฉพาะของครอบครัว
- ผู้บริโภคจะตื่นตัวและตื่นตูมกับเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์มากยิ่งขึ้น หน่วยงานและบริษัทต่างๆ จะต้องเตรียมพร้อมรับมือกับการเคลื่อนไหวของผู้บริโภคด้วยเช่นกัน

การพัฒนาเทคโนโลยี Internet of Things (IoT)

- บริษัทต่างๆ จะหันมาใช้เทคโนโลยี IoT มากยิ่งขึ้น อย่างไรก็ตาม การใช้ระบบ WiFi และ Bluetooth ซึ่งเป็นระบบสำคัญของ IoT จะเปิดช่องทางให้อาชญากรไฟเบอร์โจมตีทั้งผู้ใช้และบริษัทผู้ให้บริการได้มากยิ่งขึ้น ความเสียหายที่เกิดจากการโจมตีไซเบอร์จะมีผลถึงชีวิตมากยิ่งขึ้น เพราะเทคโนโลยี IoT จะถูกนำมาใช้กับระบบที่มีความสำคัญต่อความปลอดภัยของชีวิตมนุษย์ เช่น ระบบจราจร ระบบการแพทย์ ฯลฯ ด้วยเหตุนี้ ในปีหน้านี้บริษัทต่างๆ จะมีการลงทุนในการรักษาความปลอดภัยทางไซเบอร์มากยิ่งขึ้น

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

- โดรน (drone) จะเป็นเทคโนโลยีใหม่ที่ได้รับความนิยมใช้อย่างมากในปี พ.ศ. 2561 ไม่ว่าจะเป็นเพื่อการสำรวจ การจัดส่งสินค้าและบริการต่างๆ ฯลฯ แม้ว่า โดรนจะยังไม่ใช่เป้าหมายของอาชญากรไซเบอร์มืออาชีพ ในปีหน้า แต่เชื่อได้ว่าแฮกเกอร์มือสมัครเล่นจะเริ่มใช้โดรนเป็นหนูทดลองฝึกปรือฝีมือในการโจมตีไซเบอร์ ซึ่งผู้ใช้โดรนควรจะเตรียมรับมือไว้ด้วยเช่นกัน
- สมาร์ทโฮม เป็นอีกหนึ่งเทคโนโลยีที่จะขยายตัวสู่ตลาดผู้บริโภคมากยิ่งขึ้นในปีหน้า ไม่ว่าจะเป็นหลอดไฟ เครื่องปิ้งขนมปัง ประตู กล้อง ฯลฯ ทุกอย่างจะถูกเชื่อมโยงเข้ากับเครือข่ายคอมพิวเตอร์ แม้ว่าเทคโนโลยีเหล่านี้จะถูกสร้างขึ้นมาเพื่ออำนวยความสะดวกแก่ผู้ใช้ แต่อย่างก็ตาม เทคโนโลยีนี้จะกลายเป็นเป้าหมายของแฮกเกอร์ หากพวกเขาสามารถเจาะเข้ามาในระบบได้ ก็ไม่ต่างกับการที่มีคนแปลกหน้าเข้าไปในบ้านของคุณ และสามารถควบคุมอุปกรณ์ทุกอย่างภายในบ้านได้

ปัญหาของค่าเงินดิจิทัล (cryptocurrency)

- ค่าเงินดิจิตอลจะเป็นอีกหนึ่งเทคโนโลยีที่มาแรงในปีหน้า และขณะเดียวกันก็เป็นเทคโนโลยีตกเป็นเครื่องมือของอาชญากรไซเบอร์ เพราะด้วยความที่ค่าเงินดิจิตอลเป็นค่าเงินที่ปิดซ่อนข้อมูลของผู้รับ ผู้ส่ง และการเคลื่อนย้ายเงินทุนต่างๆ ทำให้อาชญากรไซเบอร์ใช้ค่าเงินดิจิตอลในการเรียกค่าไถ่ข้อมูล ซึ่งมีผลทำให้เกิดการแพร่ขยายของ ransomware หรือ มัลแวร์ (Malware) ประเภทหนึ่งที่มีผลจำกัดการใช้งานของผู้ใช้ (เช่น การใส่รหัสไฟล์ซึ่งอยู่ในคอมพิวเตอร์ของผู้ใช้เอง หากผู้ใช้ต้องการเรียกใช้งานไฟล์ที่ถูกโจมตี จะต้องยอมจ่ายค่าไถ่)

- ค่าเงินดิจิตอลเองก็เป็นเป้าหมายของอาชญากรไซเบอร์เช่นกัน เช่น การเปลี่ยนรหัสของผู้รับเงินให้เป็นรหัสของอาชญากร ทำให้เจ้าของเงินไม่ได้รับเงินตามที่ควร เนื่องจากมูลค่าปัจจุบันในตลาดของค่าเงินดิจิตอล (เช่น Bitcoin, Ethereum, Litecoin และ Monero) นับเป็นมูลค่าไม่ต่ำกว่า 1 พันล้านเหรียญสหรัฐฯ คาดว่าในปี 2561 ค่าเงินดิจิตอลจะเติบโตขึ้นอีก จึงทำให้การโจมตีค่าเงินดิจิตอลเป็นที่ดึงดูดใจของอาชญากรไซเบอร์ไม่น้อย

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

ไบโอแมทริกซ์ (biometrics) และ การพิสูจน์ตัวบุคคลหลายขั้นตอน (multi-factor authentication)

– หลังจากที่บริษัท Apple และ Samsung ประสบความสำเร็จในการใช้ ไบโอแมทริกซ์ (biometrics) หรือการใช้ข้อมูลทางชีวภาพ (เช่น การใช้ลายนิ้วมือ ม่านตา หรือโครงหน้า) ในการระบุตัวตนเพื่อใช้เครื่องมือสื่อสารเคลื่อนที่ต่างๆ ในปี พ.ศ. 2561 ไบโอแมทริกซ์จะถูกนำมาใช้ทดแทนการกรอกรหัสผ่าน (password) มากยิ่งขึ้น ในขณะเดียวกัน การจัดเก็บข้อมูลไบโอแมทริกซ์นั้นมีความท้าทายมากกว่าการเก็บข้อมูลส่วนตัวอื่นๆ เช่น หมายเลขบัตรเครดิต หมายเลขบัตรประจำตัวต่างๆ ฯลฯ เพราะข้อมูลหมายเลขต่างๆ มีวันหมดอายุและสามารถเปลี่ยนแปลงได้ แต่ข้อมูลไบโอแมทริกซ์จะไม่มีการเปลี่ยนแปลง เมื่อระบบได้เก็บข้อมูลไบโอแมทริกซ์ไปแล้ว ข้อมูลนั้นก็จะสามารถระบุตัวตนได้ตลอดไป

– ตลาดของเทคโนโลยีอินฟราเรดจะขยายตัวมากยิ่งขึ้น เนื่องจากการเก็บข้อมูลและการอ่านข้อมูลไบโอแมทริกซ์จะต้องการเทคโนโลยีที่ถ่ายภาพและอ่านข้อมูลได้อย่างละเอียดและแม่นยำมากยิ่งขึ้น เพื่อตอบสนองการขยายตัวของตลาดและความต้องการความปลอดภัยที่สูงขึ้น

ทิศทางมาตรการความปลอดภัยไซเบอร์

– อาชญากรไซเบอร์จะหันมาให้ความสนใจกับการโจมตีเมนเฟรม (mainframe หรือ หน่วยประมวลผลส่วนกลางของเครื่องคอมพิวเตอร์) มากขึ้น เนื่องจากความสนใจในการพัฒนาความปลอดภัยไซเบอร์ในปัจจุบันและอนาคตจะมุ่งไปที่เครื่องมือสื่อสารเคลื่อนที่และระบบ cloud ในขณะที่ เมนเฟรมเป็นศูนย์ประมวลผลที่โดยเฉพาะการประมวลผลทางการเงินให้แก่หน่วยงานระดับโลกกว่าพันแห่ง และเป็นระบบที่สนับสนุนการถ่ายโอนเงินผ่านระบบ ATM กว่า 29 ล้านครั้งต่อวันและการใช้บัตรเครดิตร้อยละ 87 ทำให้เมนเฟรมกลายเป็นจุดอ่อนและเป็นที่ดึงดูดของอาชญากรไซเบอร์

– ธุรกิจต่างๆ เริ่มหันมาใช้เทคโนโลยี Cloud และ container (Software Container เป็น concept ของการสร้างสภาพแวดล้อมเฉพาะให้ซอฟต์แวร์ทำงานได้โดยไม่กวนกับซอฟต์แวร์ตัวอื่นบนระบบปฏิบัติการเดียวกัน) มีผลทำให้ผู้ดูแลระบบต้องเชื่อมต่อระบบความปลอดภัยเข้าสู่ระบบ DevOps (DevOps คือรูปแบบวิธีการปฏิบัติ วัฒนธรรม และกระบวนการต่างๆ เพื่อแก้ไขปัญหาที่เกิดจากความขัดแย้งระหว่าง Development และ Operations) มีผลทำให้อาชญากรไซเบอร์มุ่งโจมตีไปที่ container ซึ่งจะทำได้ง่ายกว่า อย่างไรก็ตาม ผู้ดูแลระบบสามารถใช้เทคโนโลยี Deception (การใช้เหยื่อล่อ หรือเล่ห์เหลี่ยมที่ถูกออกแบบมาเพื่อขัดขวางกระบวนการทางความเข้าใจของแฮกเกอร์ หรือตรวจจับการโจมตีของแฮกเกอร์) เพื่อช่วยให้ DevOps สามารถตรวจจับการโจมตีได้รวดเร็วขึ้น

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

ไบโอแมทริกซ์ (biometrics) และ การพิสูจน์ตัวบุคคลหลากปัจจัย (multi-factor authentication)

– หลังจากที่บริษัท Apple และ Samsung ประสบความสำเร็จในการใช้ ไบโอแมทริกซ์ (biometrics) หรือการใช้ข้อมูลทางชีวภาพ (เช่น การใช้ลายนิ้วมือ ม่านตา หรือโครงหน้า) ในการระบุตัวตนเพื่อใช้เครื่องมือสื่อสารเคลื่อนที่ต่างๆ ในปี พ.ศ. 2561 ไบโอแมทริกซ์จะถูกนำมาใช้ทดแทนการกรอกรหัสผ่าน (password) มากยิ่งขึ้น ในขณะเดียวกัน การจัดเก็บข้อมูลไบโอแมทริกซ์นั้นมีความท้าทายมากกว่าการเก็บข้อมูลส่วนตัวอื่นๆ เช่น หมายเลขบัตรเครดิต หมายเลขบัตรประจำตัวต่างๆ ฯลฯ เพราะข้อมูลหมายเลขต่างๆ มีวันหมดอายุและสามารถเปลี่ยนแปลงได้ แต่ข้อมูลไบโอแมทริกซ์จะไม่มีการเปลี่ยนแปลง เมื่อระบบได้เก็บข้อมูลไบโอแมทริกซ์ไปแล้ว ข้อมูลนั้นก็จะสามารถระบุตัวตนได้ตลอดไป

– ตลาดของเทคโนโลยีอินฟราเรดจะขยายตัวมากยิ่งขึ้น เนื่องจากการเก็บข้อมูลและการอ่านข้อมูลไบโอแมทริกซ์จะต้องการเทคโนโลยีที่ถ่ายภาพและอ่านข้อมูลได้อย่างละเอียดและแม่นยำมากยิ่งขึ้น เพื่อตอบสนองการขยายตัวของตลาดและความต้องการความปลอดภัยที่สูงขึ้น

ทิศทางมาตรการความปลอดภัยไซเบอร์

– อาชญากรไซเบอร์จะหันมาให้ความสนใจกับการโจมตีเมนเฟรม (mainframe หรือ หน่วยประมวลผลส่วนกลางของเครื่องคอมพิวเตอร์) มากขึ้น เนื่องจากความสนใจในการพัฒนาความปลอดภัยไซเบอร์ในปัจจุบันและอนาคตจะมุ่งไปที่เครื่องมือสื่อสารเคลื่อนที่และระบบ cloud ในขณะที่ เมนเฟรมเป็นศูนย์ประมวลผลที่โดยเฉพาะการประมวลผลทางการเงินให้แก่หน่วยงานระดับโลกกว่าพันแห่ง และเป็นระบบที่สนับสนุนการถ่ายโอนเงินผ่านระบบ ATM กว่า 29 ล้านครั้งต่อวันและการใช้บัตรเครดิตร้อยละ 87 ทำให้เมนเฟรมกลายเป็นจุดอ่อนและเป็นที่ดึงดูดของอาชญากรไซเบอร์

– ธุรกิจต่างๆ เริ่มหันมาใช้เทคโนโลยี Cloud และ container (Software Container เป็น concept ของการสร้างสภาพแวดล้อมเฉพาะให้ซอฟต์แวร์ทำงานได้โดยไม่กวนกับซอฟต์แวร์ตัวอื่นบนระบบปฏิบัติการเดียวกัน) มีผลทำให้ผู้ดูแลระบบต้องเชื่อมต่อระบบความปลอดภัยเข้าสู่ระบบ DevOps (DevOps คือรูปแบบวิธีการปฏิบัติ วัฒนธรรม และกระบวนการต่างๆ เพื่อแก้ไขปัญหาที่เกิดจากความขัดแย้งระหว่าง Development และ Operations) มีผลทำให้อาชญากรไซเบอร์มุ่งโจมตีไปที่ container ซึ่งจะทำได้ง่ายกว่า อย่างไรก็ตาม ผู้ดูแลระบบสามารถใช้เทคโนโลยี Deception (การใช้เหยื่อล่อ หรือเล่ห์เหลี่ยมที่ถูกออกแบบมาเพื่อขัดขวางกระบวนการทางความเข้าใจของแฮกเกอร์ หรือตรวจจับการโจมตีของแฮกเกอร์) เพื่อช่วยให้ DevOps สามารถตรวจจับการโจมตีได้รวดเร็วขึ้น

ทิศทางความปลอดภัยไซเบอร์ในปี 2561

- หน่วยงานต่างๆ จะให้ความสำคัญกับการรักษาความปลอดภัยแบบ predictive security หรือ การมองหาโอกาสและความเสี่ยงที่จะถูกโจมตี แทนการรักษาความปลอดภัยแบบตั้งรับ
- เว็บไซต์ต่างๆ จะถูกอาชญากรทางไซเบอร์ใช้เป็นเครื่องมือในการเก็บซ่อน Malware ฝังรหัสที่ดึงเอาศักยภาพของคอมพิวเตอร์ของเหยื่อมาใช้ในการปั่นมูลค่าของค่าเงินดิจิทัล และการแอบขโมยข้อมูลในเครื่อง ฯลฯ
- ประเทศต่างๆ จะหันมาเก็บข้อมูลต่างๆ ในแบบ on premise (หรือ การเก็บข้อมูลในฐานข้อมูลที่ตั้งอยู่ในพื้นที่และอยู่ในการดูแลของหน่วยงานหรือประเทศ) มากยิ่งขึ้น แทนที่การเก็บข้อมูลแบบ cloud (ซึ่งข้อมูลจะถูกเก็บในฐานข้อมูลของบริษัทผู้ให้บริการซึ่งตั้งอยู่ห่างไกล และนอกเหนือการควบคุมของผู้ใช้บริการ) อย่างไรก็ตาม การเก็บข้อมูลแบบ on premise เองก็มีความเสี่ยงเช่นกัน ดังนั้นหน่วยงานจะต้องพิจารณาเลือกใช้วิธีการเก็บข้อมูลให้เหมาะสม
- ในปี พ.ศ. 2561 การโจมตีทางไซเบอร์จะมีความซับซ้อนมากยิ่งขึ้น โดยเฉพาะจากอาชญากรที่ได้รับการสนับสนุนทางการเงินจากทั้งองค์กรลับ หรือรัฐบาลของประเทศต่างๆ ก็ตาม ผู้เชี่ยวชาญบางท่านได้คาดการณ์ไว้ว่า อาชญากรไซเบอร์จะมุ่งโจมตีไปที่ผู้ให้บริการระบบ Cloud ยักษ์ใหญ่ อย่าง Amazon AWS, Microsoft Azure, และ Google's GPC และจะมีการเจาะขโมยข้อมูลมากยิ่งขึ้น

ปัญหา Gender ด้านความปลอดภัยไซเบอร์

ในปัจจุบัน มีแรงงานที่มีหน้าที่เกี่ยวกับความปลอดภัยทางไซเบอร์ที่เป็นเพศหญิงอยู่เพียงร้อยละ 11 สถานการณ์ขาดแคลนแรงงานด้านนี้ในปี พ.ศ. 2561 ถือเป็นโอกาสทองของผู้เชี่ยวชาญเพศหญิงในการเข้ามามีบทบาทในวงการความปลอดภัยไซเบอร์ นอกจากนี้ องค์กรต่างๆ จะเปิดโอกาสให้ผู้ที่มีความเชี่ยวชาญในด้านความปลอดภัยไซเบอร์ที่ไม่ได้ผ่านระบบการศึกษาแบบดั้งเดิม (เช่น ผู้ที่ศึกษาเฉพาะทางในระดับมหาวิทยาลัย) ขอเพียงผู้นั้นมีความรู้ ความเข้าใจ และสามารถแก้ไขปัญหาได้ แม้จะไม่มีใบรับรองการศึกษาเฉพาะทางก็จะเป็นที่ยอมรับมากยิ่งขึ้น บางบริษัทอาจจะหันมาสร้างผู้เชี่ยวชาญเพื่อตอบสนองความต้องการของบริษัทเอง หรือการสนับสนุนให้สังคมให้ความสนใจกับปัญหาความปลอดภัยไซเบอร์มากยิ่งขึ้น เพื่อให้มีการลงทุนในระบบการศึกษาและผลิตบุคลากรที่มีความเชี่ยวชาญในสาขานี้มากยิ่งขึ้น

กฎหมายคุ้มครองข้อมูลใน EU จะสามารถเป็นตัวอย่างให้สหรัฐฯ ได้หรือไม่

ที่มา: Alyssa Newcomb วันที่ 22 กันยายน 2560

Link: https://www.nbcnews.com/tech/security/could-europe-teach-u-s-lesson-about-cyber-regulation-n803656

กรณีศึกษาครั้งใหญ่ของประเทศสหรัฐฯ เมื่อบริษัท Equifax 1 ใน 3 บริษัทฐานข้อมูลด้านการเงินและสินเชื่อยักษ์ใหญ่ ออกแถลงการณ์ชี้แจงหลังบริษัทถูกล้วงข้อมูลโดยแฮกเกอร์ ส่งผลให้ข้อมูลส่วนบุคคล ไม่ว่าจะเป็น ชื่อ นามสกุล วันเดือนปีเกิด, Social Security Number, ที่อยู่ และอื่น ๆ ของชาวอเมริกันกว่า 143 ล้านคน และข้อมูลหมายเลขใบขับขี่ รวมไปถึงหมายเลขบัตรเครดิตของอีกประมาณ 209,000 คน รั่วไหลสู่สาธารณะ และไม่ใช่เพียงแค่ชาวอเมริกันเท่านั้นที่ได้รับผลกระทบในครั้งนี้ หากแต่ชาวอังกฤษและแคนาดาก็มีรายชื่อปรากฏอยู่ในฐานข้อมูลนี้ด้วย Equifax พบว่าระบบถูกแฮกข้อมูลในช่วงเดือนพฤษภาคม แต่ออกมาชี้แจงเมื่อวันที่ 29 กรกฎาคม 2560 ซึ่งทาง Equifax ร่วมกับหน่วยงานของสหรัฐฯ แคนาดา และอังกฤษว่าจ้างทีมงานด้านไซเบอร์เข้ามาวิเคราะห์ปัญหา รวมถึง FBI ก็เข้ามาตรวจสอบสถานการณ์ของบริษัทด้วยเช่นกัน นอกจากนี้ Equifax สร้างเว็บไซต์ชื่อ www.equifaxsecurity2017.com สำหรับให้ผู้บริโภคเข้ามาตรวจสอบว่า ข้อมูลของตนเองนั้นตกเป็นเหยื่อของการโจมตีครั้งนี้หรือไม่ รวมถึงเปิดบริการ Call Center เพื่อตอบคำถามต่างๆ แก่ลูกค้า นอกเหนือจากบริษัทยักษ์ใหญ่อย่าง Equifax ที่ถูกเจาะระบบข้อมูล ในอดีตยังมี Target และ Yahoo ที่ถูกแฮกข้อมูลและเปิดเผยในภายหลังด้วย

สำหรับในยุโรปมีการออกกฎหมายใหม่ที่เรียกว่า General Data Protection Regulation (GDPR) เป็นกฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค โดยกฎหมายฉบับนี้มีข้อกำหนดให้ธุรกิจต่างๆ โดยเฉพาะอย่างยิ่งธุรกิจบริการทางอินเทอร์เน็ตต้องปฏิบัติตามมาตรการต่างๆ ที่เพิ่มความเข้มงวดในการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค เช่น การกำหนดให้ธุรกิจใดๆ ที่มีกิจกรรมหลักเกี่ยวข้องกับการประมวลข้อมูลส่วนบุคคลของลูกค้าต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer) และการกำหนดให้ธุรกิจที่มีข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการต้องระบุเงื่อนไขการใช้งานที่เกี่ยวข้องกับสิทธิส่วนบุคคลด้วยภาษาที่ชัดเจน และเข้าใจง่ายพร้อมทั้งต้องขอรับความยินยอมจากผู้ใช้บริการในการจัดเก็บ และใช้งานข้อมูลดังกล่าว โดยธุรกิจต่างๆ ไม่สามารถสรุปจากการที่ของลูกค้าไม่โต้แย้งเงื่อนไข หรือการกรอกแบบฟอร์มยอมรับเงื่อนไขการใช้บริการให้แก่ลูกค้าล่วงหน้าว่า เป็นการให้ความยินยอมโดยลูกค้า โดยกฎหมายจะเริ่มมีผลใช้ในเดือนพฤษภาคม 2561 โดย GDPR จะครอบคลุมถึงวิธีที่บริษัทจัดเก็บข้อมูลและกำหนดให้บริษัทแจ้งเตือนภายใน 72 ชั่วโมงหลังจากมีการเจาะระบบข้อมูล หากบริษัทไม่ปฏิบัติตามข้อกำหนดจะถูกปรับ 4% ของรายได้ทั้งหมดทั่วโลก หรือ 20 ล้านยูโรโดยยึดค่าปรับจำนวนที่สูงที่สุด และที่สำคัญผลบังคับใช้จะไม่จำกัดเฉพาะบริษัทที่ตั้งอยู่ในประเทศสมาชิก EU เท่านั้น แต่จะครอบคลุมไปถึงบริษัทที่มีลูกค้าอยู่ใน EU ด้วย เพราะฉะนั้น บริษัทอเมริกันที่มีการเก็บข้อมูลของชาวยุโรปจะต้องปฏิบัติตามกฎระเบียบการป้องกันข้อมูลนี้เช่นเดียวกัน สำหรับผู้ที่ไม่มีสัญชาติยุโรปมีความเป็นไปได้ที่บริษัทเลือกที่จะปฏิบัติต่อข้อมูลของทุกคนเช่นเดียวกัน ทางด้านผู้เชี่ยวชาญการรักษาความปลอดภัยในโลกไซเบอร์ให้ความเห็นว่า ขณะที่สภาพแวดล้อมของอันตรายบนไซเบอร์กำลังพัฒนาตัวเองไปอย่างรวดเร็ว ควรมีการหารือในเรื่องกฎระเบียบที่นำมาใช้เพื่อปกป้องการคุกคามทางไซเบอร์นี้ โดยเทคนิคเดิมๆ ไม่เพียงพอที่จะให้ความปลอดภัยแก่ข้อมูลจากการโจมตีทางไซเบอร์อีกต่อไป

The Great Wall and the Great Firewall

สองกำแพงใหญ่ที่กันมิให้ศัตรูใดมารุกราน จากพระเจ้าจิ๋นซี สู่ ประธานสีจิ้น (ผิง)

ในประวัติศาสตร์ร่วมสมัย เมื่อกล่าวถึงคำว่ามหาอำนาจ คงไม่มีใครปฏิเสธว่า สหรัฐอเมริกา เป็นประเทศที่มีศักยภาพเลื่องลือที่สุดในการจัดระเบียบของโลก และเป็นผู้นำเทคโนโลยีจากห้วงอวกาศ สู่ท้องทะเลลึก จากเทคโนโลยีอาวุธยุทโธปกรณ์ ไปจนถึง เทคโนโลยีของเล่น ทิศทางของโลกที่นำโดยสหรัฐอเมริกาที่ผ่านมา จึงมุ่งมั่นหลักการเสรีนิยม และทุนนิยม ซึ่งเชื่อว่าว่าจะนำไปสู่เสถียรภาพทางการเมือง และความมั่งคั่งทางเศรษฐกิจมากที่สุด และไม่เคยมีใครสามารถมาท้าทายอำนาจของสหรัฐฯ ได้ หลังสิ้นสุดสงครามเย็น และการล่มสลายของสหภาพโซเวียต ดินแดนม่านเหล็ก จนกระทั่ง สามทศวรรษหลังที่ผ่านมา ประเทศโบราณที่เคยสร้างสิ่งมหัศจรรย์ The Great Wall ที่ยิ่งใหญ่ ที่ปิดตัวเองหลบอยู่หลังม่านไม้ไผ่ อย่างสาธารณรัฐประชาชนจีน ก็ค่อยๆ ปรากฏตัวขึ้น พร้อมกับการเลือกที่จะเดินนโยบายเศรษฐกิจแบบเปิดอย่างสหรัฐ ซึ่งถ้าเทียบอายุและการพัฒนาทางประวัติศาสตร์ จีนนับเป็นอาก๋ง ของสหรัฐฯ ได้เลย และโดยปัจจัยภายใน ไม่ว่าจำนวนประชากร แรงงานราคาถูก และการได้สิทธิประโยชน์หลายอย่างในฐานะประเทศกำลังพัฒนา ทำให้จีนค่อยๆ ก้าวขึ้นมาเป็นคู่แข่งกับสหรัฐฯ อย่างสมบูรณ์ในทุกๆ ด้าน และกลายเป็นประเทศผู้นำในด้านวิทยาการ เทคโนโลยี และนวัตกรรมต่างๆ โดยมีความแตกต่างทางนโยบายพัฒนาประเทศ คือจีนไม่ได้ปล่อยให้ทุกอย่างดำเนินไปอย่างเสรีทั้งหมด แต่รัฐบาลยังควบคุมและจ้องมอง ให้การพัฒนาเดินหน้าไปแบบรถด่วนที่ไร้แรงต้านใดๆ ซึ่งทำให้จีนได้เปรียบหลายอย่างในด้านการตลาด การควบคุมสื่อ และระบบข้อมูลข่าวสารของประเทศ

นโยบาย Great Firewall ของจีน เป็นคำที่ชาวสหรัฐฯ ใช้อุปมา นโยบายด้านการควบคุมการสื่อสารโทรคมนาคมของจีน ที่ได้นำมาใช้ในทศวรรษ 1980 หลังจากที่ท่านผู้นำหัวก้าวหน้า นายเติ้งเสี่ยวผิงกล่าวว่า “เมื่อคุณเปิดหน้าต่างรับอากาศบริสุทธิ์ มันก็ต้องมีแมลงวันบินเข้ามา” ดังนั้นในยุค 4 ทันสมัยของจีน ที่เริ่มมา

The Great Wall and the Great Firewall

ตั้งแต่ ค.ศ. 1976 เรามักจะคุ้นวลีเด็ดของท่านเติ้งที่ว่า “ไม่ว่าแมวขาวหรือแมวดำ ขอเพียงจับหนูได้ก็คือแมวที่ดี” เมื่อบวกด้วยนโยบายกั้นแมลงวันไม่ให้เข้ามากวนแมวขณะจับหนู จึงทำให้นโยบาย 4 ทันสมัยของจีนรุดหน้าไปได้อย่างรวดเร็ว ภายใต้กฎหมายความมั่นคงภายใน แม้กระทั่งอาจโดนสะกิดเรื่องสิทธิมนุษยชนไปบ้าง แต่รัฐบาลจีนก็ได้พิสูจน์ให้เห็นถึงอัตราที่ทำให้ประชาชนส่วนใหญ่มีคุณภาพที่ดีขึ้นอย่างรวดเร็ว และต่อเนื่องอย่างไม่หยุดยั้ง

อินเทอร์เน็ต ได้เข้ามายังประเทศจีนใน 2537 และรัฐบาลก็เริ่มควบคุมการไหลของข้อมูลผ่านระบบดังกล่าวในปี 2540 จีนให้ความสำคัญกับการรักษาเอกภาพและความสงบของประเทศ และยังคงต้องระมัดระวังความพยายามก่อความไม่สงบของชนกลุ่มน้อย รัฐบาลได้ป้องกันการให้ข้อมูลที่เป็นปฏิปักษ์ การบิดเบือนความจริง ข่าวลือ ลามกอนาจาร การพนัน ความรุนแรง หรือการทำร้ายระเบียบสังคม โดยมีศูนย์ควบคุมกลั่นกรองข้อมูลแบบ single gateway ที่เข้มแข็ง ในปี 2546 จีนใช้นโยบายเกราะทองคำ (Golden Shield) ที่พัฒนามาจากโปรดแกรมของบริษัท CISCO ของสหรัฐ โครงการนี้สำเร็จในปี 2549 และเป็นการสร้างยามเฝ้าประตู ไม่ให้ website ไม่พึงประสงค์หรือฝ่ายปรปักษ์ เข้ามาระคายเคืองสังคมจีน โดยเฉพาะการก่อให้เกิดการยั่วยุทางการเมืองจะถูกเพ่งเล็งเป็นพิเศษ

ในปี 2551 รัฐบาลจีนเข้าจัดการกับอินเตอร์เน็ตคาเฟ่ ที่เยาวชนเข้าไปมั่วสุมให้เป็น สิ่งผิดกฎหมาย ดังนั้น ความก้าวหน้าของจีนในทางเทคโนโลยี ไม่ได้ส่งเสริมให้เด็กจีนมีศักยภาพในการเล่นเกมส์ออนไลน์และซิ่งรถมอร์เตอร์ไซต์ ซึ่งต่างจากเด็กไทยตั้งแต่ยุค 1.0 – 4.0 อินเทอร์เน็ตคาเฟ่ทุกแห่งต้องลงทะเบียนผู้เข้าใช้ และห้ามเยาวชนต่ำกว่าอายุ 18 เข้าใช้คาเฟ่ การลงโทษไม่ได้มาลงที่เด็ก แต่จัดการกับร้าน ในขณะเดียวกันก็พัฒนามุม IT ตามเมืองใหญ่ในแนวผับและคาเฟ่หลายแห่ง เปิดโอกาศให้นักศึกษามหาวิทยาลัยได้มารวมตัวกันคิดค้นปั้นตนเองไปสู่การเป็น Start-up นโยบายจีนจึงเด่นที่กล้าที่จะโหดเหี้ยมกับสิ่งเลวร้ายและกล้าที่จะส่งเสริมกิจกรรมสิ่งดีงามสร้างสรรค์ แต่สิ่งที่ทำให้สหรัฐฯ และประเทศตะวันตกกังวล คือนโยบายดังกล่าวถือเป็นการกีดกันทางการค้า โดยเฉพาะการค้าออนไลน์ เนื่องจาก จีนได้ปิดกั้นเว็บไซต์ของต่างชาติที่จะเข้ามายังจีน ด้วยเช่นกัน และสนับสนุนให้บริษัท IT ภายในประเทศพัฒนาเว็บไซต์ที่มีศักยภาพขึ้นมารองรับความต้องการของประชาชน ดังเช่น บริษัท Alibaba ของแจ๊คหม่า หรือ บริษัท Tencent เจ้าของ Wechat

เว็บไซต์ของจีน ที่ใช้แทนเว็บไซต์ สหรัฐในจีนแผ่นดินใหญ่

Alibaba	Amazon
Baidu	Google
WeChat	WhatsApp, Line
Weibo	Facebook
You Ku	You tube
Ctrip	Orbitz, Travelocity
Mei you (ไม่มี)	Pornhub, Youporn

The Great Wall and the Great Firewall

สิ่งที่รัฐบาลจีนยังคงดำเนินนโยบายเช่นนี้ ยังคงสามารถอธิบายต่อประชาคมโลกได้ไม่ยาก สำหรับประเทศขนาดใหญ่ที่มีประชากรมากกว่า 1300 ล้าน ที่ไม่ต้องการเสี่ยงกับปัญหาความล่อแหลมทางความมั่นคงภายใน ตัวอย่างง่ายๆ อาทิ ขณะที่กฎหมายจีน มีการควบคุมการค้าการพกพาอาวุธปืนที่เคร่งครัด ในสหรัฐฯ อาวุธปืนสามารถสั่งซื้อปืนได้ออนไลน์ในสหรัฐฯ เพียงแต่ต้องไปรับสินค้าที่ Dealer เพื่อลงทะเบียน การควบคุมตลาดอาวุธปืนของจีน จึงอาจนับว่าเป็นตัวอย่างที่ดีในการคุ้มครองความสงบสุขของสังคม และแม้ว่าจีนกับสหรัฐฯ มีกฎหมายที่เข้มงวด และมีการบังคับใช้ที่ชัดเจน สิ่งที่สองประเทศก็มีการบังคับใช้ที่ต่างกัน โดยจีนมีการบังคับใช้กฎหมายอาญาได้รุนแรงแบบท่านเปาบุ้นจิ้นกับเครื่องประหาร 3 สไตล์สำหรับผู้กระทำผิดได้มากกว่า

เมื่อคำถามสำคัญที่มักถูกโยงมาหาประเด็นสิทธิมนุษยชน ถามว่าคนจีนรู้สึกอึดอัดไหม ที่ถูกบล๊อกเว็บต่างๆ คำตอบส่วนใหญ่ก็คือไม่ เพราะเว็บของจีนเองล้วนมีลักษณะที่เรียกว่าง่ายกับผู้ใช้ (user friendly) โดยเฉพาะการใช้ภาษาจีนแมนดารินเป็นหลัก ดังจะเห็นได้จากเวลาคนจีนมาเมืองไทย ซึ่งสามารถเข้าถึงเว็บไซต์ที่หลายหลาก นักท่องเที่ยวจีนก็ยังของเลือกใช้บริการอะไรๆ ที่เป็นของคนจีน โดยคนจีน และเพื่อคนจีน และเมื่อถามว่า นโยบายควบคุมปิดกั้นทาง IT ของจีนนั้น เป็นการละเมิดการค้าเสรีหรือไม่ คำตอบก็คือ ไม่แน่ เพราะสินค้าที่เสนอขายกันในเว็บไซต์ของจีน เช่น อาลีบาบานั้น ก็มีราคาถูก และจัดส่งไว มากกว่าสินค้าจากภายนอกประเทศ ดังนั้น ถ้าหากรัฐบาลจีนยังสามารถใช้นโยบายที่ไม่ทำให้ประชาชนส่วนใหญ่รู้สึกอึดอัดและสูญเสียคุณภาพชีวิตจากการปิดกั้นเหล่านี้ กฎหมายต่างๆ ที่รัฐบาลจีนตั้งขึ้นมา ก็มีความชอบธรรมสอดคล้องกับสถานการณ์ของตนเอง อย่างไรก็ตาม สำหรับชาวต่างชาติ เมื่อเข้าไปในจีน อาจจะรู้สึกอึดอัดได้ในทันที เมื่อไม่สามารถติดต่อประสานงานในช่องทางที่คุ้นเคยเดิมๆ ได้

ดังนั้น The Great Firewall จึงเป็นคำนิยามที่เหมาะสมกับนโยบายปิดกั้นการสื่อสารทางไอทีของจีน เช่นเดียวกับกำแพงเมืองจีน The Great Wall ในอดีต เพราะการรุกรานของศัตรูความมั่นคงในโลกสมัยใหม่มาได้ด้วยคลื่น ที่ยากแก่การป้องกัน แต่ก็เป็นบทพิสูจน์สำคัญว่า ในสถานการณ์ที่จีนใช้นโยบายเปิดไม่เต็มบานในการพัฒนาเศรษฐกิจและสังคมของประเทศ มาตั้งแต่การใช้นโยบาย 4 ทันสมัย ไม่ได้เป็นความคิดที่ผิดแต่อย่างใด แล้วประเทศไทยเราหล่ะ นโยบาย 4.0 จะทันสมัยได้แบบจีนในเร็ววันหรือไม่ ก็ต้องติดตามดูกันต่อไป

ลำโพงช่างพูด

ที่มา: HERB WEISBAUM วันที่ 28 พ.ย. 2560

Link: https://www.nbcnews.com/tech/security/hey-alexa-how-secure-are-voice-activated-assistants-you-n824566

Smart Speaker หรือลำโพงอัจฉริยะที่ทำงานด้วยคำสั่งเสียง ที่เราสามารถใช้ในการถาม สั่งให้ค้นหา หรือควบคุมการทำงานของอุปกรณ์อัจฉริยะ (Smart device) ต่างๆ ที่ติดตั้งภายในบ้านได้ การใช้ Smart Speaker เหล่านี้มีมากขึ้น ไม่ว่าจะเป็น Amazon's Echo หรือ Google Home จากข้อมูลของ Consumer Intelligence Research Partners ประชาชนกว่า 20 ล้านครัวเรือนในสหรัฐฯ ใช้ Smart Speaker โดย Amazon มีสัดส่วนตลาดโดยประมาณ 73% และ Google 27% ซึ่งคาดว่าในช่วงวันหยุดยาวคริสตมาสปีใหม่นี้ จะมียอดขายเพิ่มขึ้น 4.4 ล้านเครื่อง หรือประมาณ 22% จากปีที่แล้ว ปัจจุบันผู้คนสนุกกับการพูดคุยกับคอมพิวเตอร์เหมือนกัปตันเคิร์ก (Captain Kirk) ในภาพยนตร์ Star Trek แต่ทั้งนี้ กัปตันเคิร์กไม่ต้องกังวลเรื่องของแฮ็กเกอร์ แต่คนทั่วไปอย่างเรายังคงต้องคำนึงถึงความปลอดภัยในด้านนี้ เนื่องจากเทคโนโลยีอันชาญฉลาดนี้ยังคงมีช่องโหว่ในเรื่องของความเป็นส่วนตัวและความปลอดภัยของข้อมูลส่วนบุคคล เช่น รายชื่อที่มีการติดต่อ หรือข้อมูลบัญชีธนาคาร เป็นต้น

แม้ว่าผู้ใช้จะต้องใช้คำสั่งปลุก โดยพูด "Alexa" หรือ "OK Google" เพื่อเปิดใช้งาน ซึ่งอุปกรณ์อัจฉริยะเหล่านี้ตั้งใจฟังคำสั่งตลอดเวลา ไม่มีคำว่าหูทวนลม ซึ่งการปลุกอุปกรณ์โดยไม่ตั้งใจจึงเกิดขึ้นเป็นเรื่องธรรมดา เคยมีกรณีตัวอย่างเกิดขึ้นเมื่อต้นปี 2559 เด็กหญิงอเมริกันอายุ 6 ปี จากเมือง Dallas รัฐ Texas สั่งซื้อบ้านตุ๊กตาและคุ้กกี้ราคา 170 เหรียญสหรัฐฯ ผ่าน Alexa เนื่องจากมีการเซ็ตระบบการซื้อเปิดไว้ตั้งแต่ต้น นอกจากนี้ ไม่ว่าจะเป็นรายการวิทยุ โทรทัศน์ หรือวิดีโอ ก็สามารถเปิดการใช้งานอุปกรณ์เหล่านี้ได้เช่นกัน Burger King ได้ออกแบบโฆษณาออกมาเพื่อปลุก Google Home โดยนักแสดงในโฆษณาพูดว่า “OK Google, what is the Whopper burger?" ซึ่งในหลายกรณีมีการปลุกอุปกรณ์เหล่านี้โดยบังเอิญซึ่งอาจจะไม่ได้เป็นเรื่องใหญ่ แต่สิ่งที่ควรทราบไว้คือ เมื่ออุปกรณ์ดิจิตอลเหล่านี้ถูกปลุกให้ตื่นขึ้นแบบเฟอร์บี้ ก็จะมีการบันทึกสิ่งที่ได้มีการพูดและส่งข้อมูลการบันทึกนั้นเป็นรหัสไปยังเซิร์ฟเวอร์เพื่อจัดเก็บไว้ แต่ทั้งนี้ ผู้ใช้สามารถที่จะเปิดฟังส่วนที่มีการบันทึกหรือสามารถที่จะลบทิ้งได้ ซึ่งหากคุณมีอุปกรณ์เหล่านี้ คุณควรลองเปิดฟังแล้วจะประหลาดใจกับสิ่งที่ได้ยิน นอกจากนี้

ที่มา: https://developer.amazon.com/echo

นาย Candid Wueest นักวิจัยจากบริษัท Symantec ซึ่งเป็นบริษัทที่ดูแลความปลอดภัยของระบบดิจิทัล กล่าวถึงอันตรายที่อาจเกิดขึ้นจากการฟังตลอดเวลาของอุปกรณ์เหล่านี้ว่า แฮ็กเกอร์สามารถเจาะเข้าระบบอุปกรณ์เหล่านี้จากระยะไกลแล้วสามารถเปลี่ยนให้เป็นอุปกรณ์ในการรับฟัง และอุปกรณ์บางรุ่นยังมาพร้อมกับกล้อง ซึ่งแฮ็กเกอร์สามารถเห็นสิ่งที่คุณกำลังทำอยู่ ซึ่งเป็นเรื่องที่น่ากลัวหากมีคนอื่นที่สามารถควบคุมระบบอุปกรณ์ดิจิทัลเหล่านี้ได้ในขณะที่เราเข้าห้องน้ำหรือกำลังนอนหลับอยู่

นอกจากนี้ ลำโพงอัจฉริยะยังถูกออกแบบให้เป็นศูนย์กลางที่สามารถควบคุมและสื่อสารกับอุปกรณ์อินเทอร์เน็ตอื่นๆ (Internet of Things: IoT) ในบ้าน เช่น การปิด-เปิดไฟ การควบคุมอุณหภูมิภายในบ้าน การล็อกประตู เป็นต้น ซึ่งความสะดวกสบายใหม่ๆ เหล่านี้ มาพร้อมกับภัยคุกคามทางด้านดิจิทัลเช่นเดียวกัน ผู้ร้ายสามารถตะโกนสั่ง "เปิดประตูหน้า" และ "ปิดระบบเตือนภัย" ได้ง่ายโดยไม่ต้องอาศัยวลี Open Sesame แบบเรื่องอาลีบาบา หากอุปกรณ์เหล่านี้มีการเชื่อมต่อกับลำโพงอัจฉริยะ ซึ่งทาง Amazon กล่าวว่าได้ให้ความสำคัญในเรื่องของความปลอดภัยของลูกค้าอย่างจริงจัง ได้มีการตรวจสอบเพื่อให้การใช้ Echo มีความปลอดภัย ในส่วนของ Google ได้กล่าวถึงอุปกรณ์ทั้งหมดที่มีระบบ Google Assistant ได้มีการออกแบบให้มีความปลอดภัยและมีความเป็นส่วนตัว นอกจากนี้ ผู้ใช้ยังสามารถตรวจสอบการใช้งานของตนเองจาก Security Checkup ได้ตลอดเวลา และสามารถล็อคอินเข้าเช็คใน My Activity เพื่อลบการค้นหาประวัติการเข้าชมและกิจกรรมอื่นๆ ที่ผ่านมาจาก Google Account ได้ หากเปรียบเทียบอุปกรณ์เหล่านี้ยังไม่มีความเสี่ยงมากเท่ากับสมาร์ทโฟนหรือแล็ปท็อป แต่ทั้งนี้ผู้ใช้ควรป้องกันความเสี่ยงที่อาจจะเกิดขึ้น โดยตั้งรหัสผ่านที่คาดเดายาก และปิดใช้อุปกรณ์เมื่อไม่มีคนอยู่บ้าน เป็นต้น

ที่มา: https://store.google.com/

จากภาพยนตร์ SCI-FI ถึงความหมาย ว.ท.น.

Cyber Bully Cyber Security

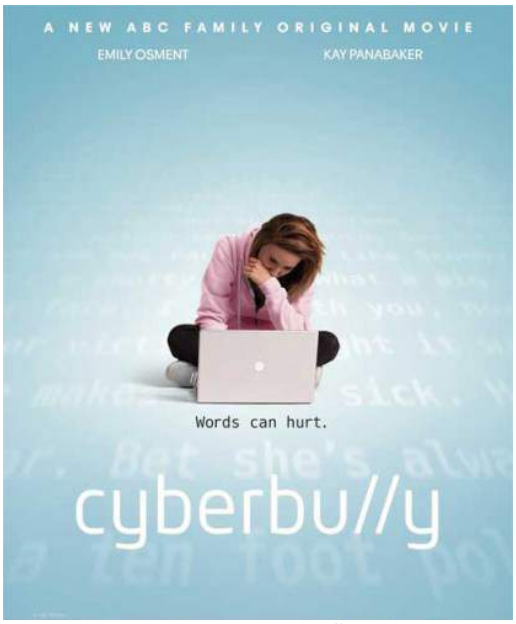
จากภาพยนตร์เกี่ยวกับ Cyber ที่มีมากมายในตลาด ที่เค้าโครงเรื่องไม่ค่อยได้เน้นตัวเทคโนโลยีมากเท่ากับการก่ออาชญากรรมและต่อสู้กับแผนการณ์ชั่วร้ายของคนที่ใช้ วทน. ด้าน Cyber ทำร้ายผู้อื่นหรือ ประเทศชาติ ไม่ว่าจะเป็นเรื่อง The Net, Die Hard IV, Enemy of State, Citizenfour โดยตัวโกงประกอบอาชีพชนิดหนึ่งที่เรียกว่า Hackers คือ พวกที่เข้าไปฉวย ฉก ยึด ล้วงฐานข้อมูลคนอื่น พร้อมกระทำการมิดีมิร้าย ช่วงชิง หน่วงเหนี่ยว กักกัน ทำลาย รวมทั้งจับเป็นสิ่งประกันเพื่อเรียกค่าไถ่ ความสนใจต่างๆ มักถูกมองไปในมิติของความมั่นคงทางการเมือง ทางทหาร และความมั่นคงทางการค้าและเศรษฐกิจ แต่ความน่ากลัวของปัญหา Cyber Security ไม่ได้มีเพียงแค่นั้น โดยเฉพาะเมื่อเรามองว่าเยาวชน คือ หัวใจของการพัฒนาโลก ภาพยนตร์เรื่อง “ฉลาด-เกมส์โกง” ของไทยที่โด่งดัง ก็เป็นภาพยนตร์เรื่องหนึ่งที่สะท้อนการนำเทคโนโลยีการสื่อสารมาประกอบอาชญากรรมของหมู่เยาวชน และการก่ออาชญากรรมไซเบอร์นั้นกลายเป็น State-of-the-Art ระดับแนวหน้าในโลกปัจจุบัน เมื่อมนุษย์สามารถนำเทคโนโลยีมาประกอบกับกระบวนการคิดของตนเองเพื่อให้ได้มาซึ่งผลลัพธ์ที่ตนเองต้องการ ปรากฏการณ์ในเกิดขึ้นในเรื่องฉลาดเกมส์โกง ถึงแม้จะมีความไม่เหมาะสมปนอยู่ แต่ในอีกมุมของเยาวชนในต่างประเทศ เหตุการณ์ที่เกิดขึ้นอาจรุนแรงกว่านั้น โดยเฉพาะการเป็นสังคมของการเคารพสิทธิส่วนบุคคล และทุกคนต้องพูดด้วยตัวเอง ไม่มีใครส้ม ใครเผือก เด็กในสังคมฝรั่งส่วนใหญ่เมื่อถูกคุกคามจึงมักมีความเปราะบางในการแก้ปัญหาแบบสังคมขี้เม้าแบบไทยๆ และตะวันออก ภาพยนตร์เรื่อง Cyberbully ที่ฉายออกมาเมื่อปี ค.ศ.2511 เป็นภาพยนตร์ที่สะท้อนให้ความหมายโดยตรงของความขัดแย้งระหว่างเยาวชนในยุคไฮเทค หรือ เด็กแกล้งเด็กผ่านเน็ต โดยที่ใช้เครื่องมือสื่อสารอย่างโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ เชื่อมต่อเครือข่ายสังคมออนไลน์ ไม่ว่าจะเป็นเฟสบุ๊ค, ทวิตเตอร์, อินสตาแกรม, แชท หรือเว็บไซต์ต่าง ๆ เป็นเครื่องมือหลักในการรังแกและกลั่นแกล้งกัน โดยการกลั่นแกล้งนี้สามารถทำได้ตลอด 24 ชั่วโมง โดยผู้กลั่นแกล้งหรือผู้เข้าชมก็สามารถนั่งชมนั่งอ่านจากมุมใดของโลกก็ได้

จากภาพยนตร์

SCI-FI

ถึงความหมาย ว.ท.น.

ภาพยนตร์เรื่องนี้ เป็นเหตุการณ์ที่เกิดขึ้นกับเด็กผู้หญิงโรงเรียนมัธยม ที่ได้รับของขวัญวันเกิดเป็นคอมพิวเตอร์โน้ตบุ๊ค และก็เข้าเป็นสมาชิก website ที่ชื่อว่า Cliquesters ที่สามารถสร้างข้อมูลตนเองและคุยกับคนอื่นได้แบบเฟสบุ๊ค, ทวิตเตอร์ ด้วยความหมั่นไส้ของเพื่อนซี้ และความเกลียดชังของคู่อริ ทำให้เธอตกเป็นเหยื่อของการถูกประณามในสังคมออนไลน์ โดยเธอก็พยายามแก้ปัญหาของเธอไปด้วยตนเอง จนเกือบจะเอาชีวิตไม่รอด ด้วยข้อครหาของการเป็นเด็กสำส่อนและมีโรคทางเพศสัมพันธ์ (ซึ่งถ้าเป็นโรงเรียนไทย เพื่อนคงฟ้องครู ครูคงเรียกผู้ปกครองมาพบ และปัญหาคงจบได้ไม่ยาก) แต่สำหรับฝรั่งแล้วคำว่า None of your business กับคำว่า Free of Speech ทำให้คนที่ไม่เข้มแข็งพอมีความล่อแหลมต่อการทำร้ายตนเองสูง เนื่องจากหากคนผู้นั้นไม่เปิดโอกาสให้ใครช่วย เขาก็ต้องจัดการกับปัญหาด้วยตนเอง ในจุดเปลี่ยนของเรื่องเมื่อเธอเลือกที่จะจบชีวิตด้วยการกินยาเกินขนาด ทำให้เพื่อนรักของเธอที่เป็นต้นตอของการก่อเรื่องได้หันมาสารภาพผิด และเมื่อผ่านเหตุการณ์เลวร้าย เธอก็ได้เข้าใจความรักของแม่ที่มีให้เธอ และเลือกที่จะเปิดใจรับฟังคำแนะนำของบุพการี โดยการเข้าไปร่วมกลุ่มที่ปรึกษาปัญหา Cyber bully ซึ่งเธอได้พบคนจำนวนมากมีปัญหาเดียวกับเธอ วลีสำคัญที่น่าสนใจเมื่อเรื่องดำเนินถึงตอนนี้ คือ อย่าซ่อนตัวอยู่หลังความกลัว “ Don’t hide behind your fear” ที่ทำให้เด็กสาวเลือกที่จะต่อสู้ตามวิธีและทางเลือกแบบที่สังคมฝรั่งเขาใช้ และในที่สุดผู้คนก็ค่อยๆ เข้าใจและหันมาเข้าข้างเธอ พร้อมกับ ชัยชนะที่ได้สอนให้ตัวอิจฉาว่า การด่าว่าคนอื่นในช่องทางสาธารณะเป็นสิ่งที่ร้ายแรงเช่นไร โดยพ่อของ Lindsay ตัวอิจฉา ซึ่งเป็นนักกฎหมาย ก็เคยดีเฟนด์ให้กับลูกสาวของเขาว่าเธอมีสิทธิใน Free of Speech โดยไม่สนใจที่จะแก้ไขปัญหาดังกล่าว



หลังจากภาพยนตร์เรื่องนี้ฉายแล้ว ได้กระตุ้นให้สหรัฐอเมริกาออกกฎหมายรองรับและจัดการเกี่ยวกับความผิดว่าด้วย Cyber bullying 34 รัฐ ในปี ค.ศ. 2011 และในปัจจุบันทุกรัฐมีกฎหมายที่เกี่ยวข้องกับกรณี Cyber bullying อย่างน้อยก็ช่วยป้องกันการทำร้ายกันทางวจีกรรมบนโลก Cyber ในสังคม Free of Speech ความน่ากลัวในโลก Cyber สำหรับเยาวชนไม่ได้จบแค่นั้น ล่าสุด The Dark Overlord ซึ่งเป็นกลุ่มแฮกเกอร์ที่เคยพยายาม รีดไถ Netflix และ ABC News มาก่อนหน้านี้ มีการส่งข้อความรีดไถหรือข่มขู่โดยมุ่งเป้าหมายไปยังโรงเรียนในเขตต่างๆ เช่น ในเมือง Johnston รัฐ Iowa เมือง Flathead County และ Columbia Falls รัฐ Montana โดยแฮกเกอร์มุ่งเป้าหมายไปยังโรงเรียนที่มีระบบการรักษาความปลอดภัยในโลกไซเบอร์ที่ไม่รัดกุมมากนัก เพื่อขโมยข้อมูลสำคัญของนักเรียนและคณาจารย์ เช่น ชื่อ ที่อยู่

เบอร์โทรศัพท์ ข้อมูลทางการแพทย์ การศึกษา และการลงโทษทางวินัย เป็นต้น และยังแฮกกล้องรักษาความปลอดภัยของโรงเรียนเพื่อดูความเคลื่อนไหวที่เกิดขึ้นภายโรงเรียนอีกด้วย โดยแฮกเกอร์เรียกร้องให้มีการจ่ายเงินในรูปแบบบิตคอยน์ (Bitcoin) หรือรูปแบบอื่นๆ เพื่อแลกกับการไม่เผยแพร่ข้อมูลส่วนบุคคลเหล่านี้ ซึ่งในปีนี้ปีเดียวมีการข่มขู่โรงเรียนกว่า 30 แห่ง โดยหลายโรงเรียนถึงกับต้องจัดสรรงบฉุกเฉินมาแก้ไขปัญหา เช่น โรงเรียนใน Horry County มลรัฐเซาท์ แคโรไลน่า ยินยอมจ่ายเงินจำนวน 10,000 เหรียญสหรัฐฯ โรงเรียนใน Fulton County มลรัฐจอร์เจีย ยอมจ่ายเงิน 75,000 เหรียญสหรัฐฯ หลังจากที่ถูกหลอกลวงให้เข้าสู่ระบบผ่านอีเมล์ปลอมเป็นต้น ในขณะที่บางโรงเรียน เช่น Columbia Falls High School ได้พูดคุยกับครอบครัวของนักเรียนและหารือร่วมกับ FBI ก่อนการตัดสินใจที่จะไม่จ่ายเงินใดๆ ให้กับแฮกเกอร์ ทำให้ได้รับข้อความข่มขู่ที่รุนแรงขึ้น ซึ่งทางด้านกระทรวงศึกษาธิการสหรัฐฯ ขอให้ทางโรงเรียนมีการดำเนินการตรวจสอบระบบความปลอดภัยและมีการฝึกอบรมบุคลากรทางด้านระบบความปลอดภัยโลกไซเบอร์ เพื่อป้องกันและหลีกเลี่ยงการตกเป็นเป้าหมายของแฮกเกอร์ ซึ่งอาจจะเป็นเรื่องที่โรงเรียนมองข้ามไปในการจัดสรรงบประมาณ นอกจากนี้ ในส่วนของ FBI กำลังพยายามตรวจสอบภัยคุมคามด้านไซเบอร์ที่เกิดขึ้นในโรงเรียนอย่างจริงจัง และแนะนำว่าไม่ควรจ่ายเงินใดๆ ให้กับอาชญากรด้านไซเบอร์เหล่านี้ เนื่องจากจะเป็นการเพิ่มความเสี่ยงในการถูกโจมตีต่อไป และจะเป็นการสนับสนุนกิจกรรมที่ผิดกฎหมาย

ภาพยนตร์สารคดี Citizenfour ซึ่งเป็นเรื่องราวของ Edward Snowden (เอ็ดเวิร์ด สโนว์เดน) อดีตลูกจ้างระดับสูงของรัฐบาลในหน่วยงาน Intelligence Community สำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา (NSA) และกลายมาเป็นบุคคลผู้สร้างประเด็นสำคัญที่สุดในด้าน Cyber Security เมื่อเขาเปิดโปงโครงการการสอดส่องดูแลมวลชนลับสุดยอดของรัฐบาลสหรัฐฯ และอังกฤษ และให้เห็นปัญหาว่าข้อมูลส่วนตัวของเรา มันมีความสำคัญมากขนาดไหน ไม่ว่าจะเป็น เลขประจำตัว บัตรเครดิต หมายเลขโทรศัพท์มือถือ อีเมล์ เพราะในกลไกในโลกยุคไซเบอร์นี้ สามารถเข้าถึงและเชื่อมโยงต่างๆ ด้วยกันได้ นั่นหมายความว่าสามารถระบุตัวตนคน ๆ หนึ่ง พฤติกรรม การติดต่อกับบุคคลอื่น ตำแหน่งที่อยู่ สินทรัพย์ รวมไปถึงการใช้งานอินเทอร์เน็ตที่เก็บรวบรวมข้อมูลไว้ ดังนั้น เยาวชนของฝรั่งจึงถูกฝึกให้เก็บความลับทางอัตลักษณ์ของตนเองไว้อย่างดีที่สุด การส่งรายงาน เขียนชื่อ (อาจชื่อเล่นย่อก็ได้) โดยให้ข้อมูลน้อยนิดที่คุณครูสามารถใช้ในการให้คะแนนได้ ในขณะที่เยาวชนไทย การวัดผลคะแนนอย่างหนึ่งจะมอบให้กับความสะอาดเรียบร้อย สวยงาม ข้อมูลครบ ลงรายละเอียดเลขที่ เลขประจำตัว พร้อมเข้าปกกระดาษหนังช้างร้อยด้วย กระดูกงู) ภาพยนตร์ Cyber จำนวนมากหลายเรื่องเกิดจากแรงบันดาลใจเหตุการณ์จริง และเตือนให้สังคมที่กำลังพัฒนา ไปในแนว 4.0 ทั้งหลาย ระมัดระวังการใช้งานอินเทอร์เน็ต หรือ Cyber กันมากขึ้น เพราะในปัจจุบัน ชีวิตปัจจุบันเราถูกผูกไว้กับเทคโนโลยีไซเบอร์อย่างดิ้นไม่หลุด และอาจถูกอาชญากรรุกรามเมื่อไหร่ก็ได้เช่นกัน