คำแปลการบรรยายทางวิชาการ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของศาลยุติธรรมสิงคโปร์และศาลปกครองไทย*

จากการที่ประเทศไทยได้มีการพัฒนาระบบเทคโนโลยีสารสนเทศซึ่งเป็นระบบที่มีการนำเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายไซเบอร์ มาใช้เพื่อการรับส่งและประมวลผลข้อมูลที่สำคัญในเกือบทุกระบบของการทำงานในช่วงหลายปีที่ผ่านมา เพื่อสนองตอบต่อนโยบายที่สำคัญของรัฐบาล ซึ่งการดำเนินงานทั้งภาครัฐและภาคเอกชนล้วนแล้วแต่มีความเกี่ยวพันกับการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญในทุกกระบวนการ แต่ในขณะที่มีการพัฒนาในด้านดังกล่าวขึ้นอย่างมากมายนั้น ก็มีความท้าทายใหม่ ๆ อันเกิดจากภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นด้วยเช่นกันในทุกภาคส่วน ไม่ว่าจะเป็นหน่วยงานภาครัฐ หรือภาคเอกชน โดยเฉพาะภัยคุกคามทางไซเบอร์ในลักษณะการหลอกลวงกับประชาชนโดยตรงนับวันจะทวีความรุนแรงมากขึ้น รัฐบาลไทยจึงต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) เพื่อใช้เป็นกรอบแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยนำมาสู่การตรากฎหมายและจัดตั้งองค์กรผู้รับผิดชอบในการดำเนินมาตรการและการประสานงานในลำดับต่อมา

ปัจจุบันระบบเทคโนโลยีสารสนเทศนอกจากมีบทบาทสำคัญที่เข้ามาช่วยอำนวยความสะดวกในการบริหารงาน และดำเนินงานขององค์กรในส่วนของการทำธุรกรรมทางอิเล็กทรอนิกส์ทั่วไปแล้ว ในส่วนของการดำเนินคดีปกครองของศาลปกครอง ได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินการเพื่อความสะดวกและรวดเร็วในการอำนวยความยุติธรรมต่อคู่กรณีด้วย โดยจัดให้มีการดำเนินคดีปกครองทางระบบอิเล็กทรอนิกส์ เพื่อให้เป็นช่องทางเลือกในการยื่นรับ-ส่งคำคู่ความ เอกสาร และคำสั่งศาลทางระบบอิเล็กทรอนิกส์ระหว่างศาลและคู่กรณีให้เป็นไปด้วยความสะดวกและรวดเร็ว

---

* สรุปความจากการอภิปรายทางวิชาการหัวข้อ “ความมั่นคงปลอดภัยทางไซเบอร์กับระบบ e-Court” เมื่อวันที่ 21 พฤษภาคม 2567 โดยสำนักงานศาลปกครองร่วมกับศาลยุติธรรมสิงคโปร์ ภายใต้กรอบความร่วมมือระหว่างหน่วยงานราชการไทย-สิงคโปร์ (Thailand-Singapore Civil Service Exchange Program – CSEP) จัดการอภิปรายทางวิชาการดังกล่าว ณ อาคารศาลปกครอง ผ่านระบบการประชุมทางไกลผ่านจอภาพ ทั้งนี้ วิทยากรฝ่ายไทย ได้แก่ ดร.ชัยภัทร ทั่งทอง และ ดร.ชาญวิทย์ ชัยกันย์ ตุลาการศาลปกครองระยอง และวิทยากรฝ่ายสิงคโปร์ คือ Mr. Toh Kon Sing, Ministry Family Chief Information Officer, Office of Transformation and Innovation โดยมีนายคติพจน์ สินสูงสุด พนักงานคดีปกครองปฏิบัติการ กลุ่มศึกษากฎหมายมหาชน 2 สำนักวิจัยและวิชาการ และนายณัฐภัทร ประเสริฐวิทย์ พนักงานคดีปกครองปฏิบัติการ กลุ่มศึกษากฎหมายมหาชน 3 สำนักวิจัยและวิชาการ ปฏิบัติหน้าที่ล่ามและจัดทำสรุปการบรรยายของวิทยากรฝ่ายสิงคโปร์

ถอดความและเรียบเรียงโดย ดร.ชัยภัทร ทั่งทอง และ ดร.ชาญวิทย์ ชัยกันย์ ตุลาการศาลปกครองระยอง

แทนการยื่นส่งเอกสารด้วยตนเองหรือทางไปรษณีย์ลงทะเบียน และเพื่อให้มีการจัดเก็บข้อมูลทางคดีในระบบอิเล็กทรอนิกส์ นอกจากนั้นแล้ว ยังจัดให้มีระบบการดำเนินกระบวนพิจารณาของศาลและคู่กรณีผ่านการประชุมทางจอภาพ เพื่อให้ศาลสามารถดำเนินกระบวนพิจารณาในการไต่สวน การนั่งพิจารณาคดี และการอ่านคำพิพากษาหรือคำสั่งของศาล โดยการเชื่อมสัญญาณสื่อสารจากศาลไปยังสถานที่ทำงานหรือที่พักอาศัยของคู่กรณีได้ อันเป็นการลดข้อจำกัดในการเดินทางหรือในสถานการณ์บ้านเมืองที่ไม่ปกติด้วยปัญหาการระบาดของโรคติดต่อดังที่ผ่านมา

แต่แม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในกิจการด้านต่าง ๆ รวมถึงการอำนวยความยุติธรรมของศาลแก่ประชาชนก็ตาม แต่ในขณะเดียวกันก็มีความเสี่ยงสูงที่อาจก่อให้เกิดความเสียหายของข้อมูลและการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานต่าง ๆ และระบบอินเทอร์เน็ต ทำให้มีโอกาสที่จะมีภัยคุกคามแฝงเข้ามาบุกรุกระบบคอมพิวเตอร์และระบบไซเบอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้ายหรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ตเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการดักหรือได้ไปซึ่งข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก ดังนั้น ผู้ใช้งานและผู้ดูแลระบบด้านเทคโนโลยีสารสนเทศจึงต้องตระหนักถึงการใช้งานและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มากเป็นพิเศษ

คงเป็นที่ยอมรับกันว่า ในยุคนี้ภัยคุกคามทางไซเบอร์กลายเป็นเรื่อง New Normal ในประเทศไทยและนานาประเทศไปแล้ว ทุกคนจึงต้องพร้อมรับมือกับภัยไซเบอร์จู่โจมที่อาจเกิดขึ้นกับทุกคนได้ทุกเมื่อ ไม่ว่าจะเป็นหน่วยงานของรัฐ ศาล และองค์กรภาคเอกชน หรือบุคคลทั่วไปที่ใช้ระบบสารสนเทศ หรือคอมพิวเตอร์ในรูปแบบต่าง ๆ ผู้บริหารของทุกภาคส่วนจึงจำเป็นต้องปรับเปลี่ยนแนวคิดใหม่ในการรับมือกับภัยคุกคามทางไซเบอร์ จากแนวคิดที่ว่า “ก่อนถูกโจมตีเราจะป้องกันอย่างไร” เป็นว่า “หากถูกโจมตีเราจะรับมืออย่างไร” อันเป็นเรื่องของความสามารถในการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ เพื่อให้ธุรกิจการงานต่าง ๆ ที่ต้องพึ่งพาอาศัยระบบไซเบอร์สามารถดำเนินกิจการต่อไปได้ ซึ่งเป็นแนวคิดที่จะต้องเปลี่ยนจาก Cyber security ไปเป็น Cyber Resilience[1] อันเป็นแนวคิดที่ต้องพัฒนาไปอีกขั้น เพื่อให้ทันกับพัฒนาการของภัยคุกคามไซเบอร์ที่เปลี่ยนไปอย่างรวดเร็ว

สำหรับประเทศไทยนั้น ได้มีการตรากฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ประกอบด้วยกฎหมาย 2 ฉบับ ฉบับแรก พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) โดยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของรัฐ

[1] กรกัญญ์ญารัก บุญสุขเกิด, “สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย,” วารสารอาชญาวิทยาและสังคมศาสตร์ ปีที่ 3 ฉบับที่ 1, 2564, น. 33 (42).

และความสงบเรียบร้อยของประเทศ รวมทั้งการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง เพื่อพัฒนาความรู้ความสามารถของบุคลากร ผู้เชี่ยวชาญ และพนักงานเจ้าหน้าที่ให้มีความพร้อมในการปฏิบัติงาน และฉบับที่สอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับปกป้องข้อมูลส่วนบุคคลของประชาชน นอกเหนือจากการมีกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แล้ว ประเทศไทยยังมีกฎหมายที่เกี่ยวกับมาตรการในการป้องกัน ปราบปราม และดำเนินคดีกับผู้กระทำผิดหรือก่ออาชญากรรมทางไซเบอร์อีกหลายฉบับ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เป็นต้น ซึ่งจากการศึกษาในภาพรวมน่าจะถือได้ว่า กฎหมายของประเทศไทยได้วางบทบัญญัติเกี่ยวกับการแก้ไขรับมือปัญหา และการปราบปรามการกระทำความผิดดังกล่าวได้ในระดับเดียวกับนานาอารยประเทศ ส่วนการที่หน่วยงานต่าง ๆ ของไทยจะสามารถดำเนินการตามมาตรการที่กฎหมายกำหนดไว้ได้อย่างมีประสิทธิภาพแค่ไหนเพียงใด คงเป็นเรื่องที่ต้องติดตามกันต่อไป

กรณีอาชญากรรมทางเทคโนโลยีของประเทศไทยนั้น เมื่อวันที่ 30 ธันวาคม 2566 สำนักงานตำรวจแห่งชาติได้แถลงสถิติคดีอาชญากรรมทางเทคโนโลยี ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 20 ธันวาคม 2566 จากระบบรับแจ้งความออนไลน์ (www.thaipoliceonline.go.th) ว่า ในช่วงเวลาดังกล่าวมีการรับแจ้งความในคดีออนไลน์ จำนวนทั้งสิ้น 391,631 คดี มูลค่าความเสียหายรวมกว่า 10,122,822,746 บาท สถิติคดีออนไลน์ที่มีการรับแจ้งความมากที่สุด 5 อันดับ ได้แก่ 1. หลอกลวงซื้อขายสินค้าหรือบริการ 2. หลอกให้โอนเงินเพื่อทำงาน 3. หลอกให้กู้เงิน 4. หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ 5. ข่มขู่หลอกลวงทางโทรศัพท์ (Call Center) อย่างไรก็ตาม สถานการณ์การหลอกลวงทางออนไลน์ปรับตัวดีขึ้นบ้าง หลังจากที่ภาครัฐได้มีการประชาสัมพันธ์ให้ประชาชนรับรู้ถึงกลลวงของมิจฉาชีพและออกกฎหมายที่เข้มงวดเพื่อจัดการกลุ่มมิจฉาชีพ เช่น การจัดการบัญชีม้า ซิมผี และ SMS ปลอม เป็นต้น นอกจากนี้ ธนาคารแห่งประเทศไทยได้ออกประกาศห้ามสถาบันการเงินส่งลิงก์แนบไปยังผู้ใช้ และปรับปรุงระบบการโอนเงินโดยใช้การสแกนใบหน้าอีกด้วย[2]

ปัจจุบันศาลยุติธรรมได้มีประกาศคณะกรรมการบริหารศาลยุติธรรม ลงวันที่ 13 มีนาคม 2567 จัดตั้งแผนกคดีอาชญากรรมทางเทคโนโลยีในศาลอาญา เพื่อให้มีผู้พิพากษาที่มีความรู้ความเชี่ยวชาญในการดำเนินคดีอาชญากรรมทางเทคโนโลยี รวมทั้งมีอำนาจในการพิจารณาและสั่งคำร้องของพนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างรวดเร็วและทันท่วงที

[2] คดีโกงออนไลน์พุ่ง ! 10 เดือน-เกือบ 4 แสน เสียหายนับหมื่นล้าน ตุ๋นขายของมากสุด, ไทยรัฐออนไลน์ [ออนไลน์], เข้าถึงจาก https://www.thairath.co.th/news/crime/2751709 เมื่อ 31 ธันวาคม 2566.

สำหรับสถานการณ์ของภัยคุกคามทางไซเบอร์ในประเทศไทยนั้น แม้ไม่ปรากฏข้อมูลที่สำรวจแยกแยะจำนวนการดำเนินคดีอาญากับผู้กระทำผิดประเภทนี้ชัดเจนนัก แต่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช. : NCSA) ได้ทำการสำรวจสถิติภัยคุกคามทางไซเบอร์ในประเทศไทยในช่วงสามปีที่ผ่านมา โดยในปี พ.ศ. 2566 (มกราคม – ธันวาคม 2566) ได้จำแนกสถิติภัยคุกคามทางไซเบอร์ในประเทศไทยเป็นประเภทรูปแบบภัยคุกคามและประเภทของหน่วยงานที่ถูกโจมตี ดังนี้[3]

สถิติภัยคุกคามทางไซเบอร์ : ประเภทรูปแบบภัยคุกคาม (ปี พ.ศ. 2566)

ลำดับ	รูปแบบภัยคุกคาม	จำนวนครั้ง
1	Hacked Website (Gambling)	515
2	Hacked Website (Defacement)	336
3	Fake Website	301
4	จุดอ่อนช่องโหว่	228
5	Finance Scam – หลอกลวงการเงิน Online	112
6	Data Leak	100
7	DDoS	33
8	Hacked Website (Phishing)	38
9	Data Breach	47
10	Ransomware	27
11	Hacked Website (Malware)	12
12	Privileged account Compromise	19
13	Command and Control Server	6
14	Unauthorised access to information	6
15	Security Misconfiguration	4
16	Application Compromise	1
17	Mail Phishing	1
18	Malware	1
19	Unauthorised modification of information	1
20	อื่นๆ	1
	รวม	**1,789**

[3] สกมช., สถิติภัยคุกคามทางไซเบอร์, [ออนไลน์], เข้าถึงจาก https://www.ncsa.or.th/service-statistics.html เมื่อ 24 เมษายน 2567.

สถิติภัยคุกคามทางไซเบอร์ : ประเภทหน่วยงานที่ถูกโจมตี (ปี พ.ศ. 2566)

ลำดับ	หน่วยงานที่ถูกโจมตี	จำนวนครั้ง
0	หน่วยงานของรัฐ ด้านอื่นๆ	461
1	ความมั่นคง	77
2	บริการภาครัฐ	40
3	การเงินการธนาคาร	145
4	เทคโนโลยีสารสนเทศและโทรคมนาคม	19
5	ขนส่งและโลจีสติกส์	23
6	พลังงานและสาธารณูปโภค	74
7	สาธารณสุข	67
8	อื่นๆ	20
8.1	การศึกษา	632
8.2	ผู้ประกอบการธุรกิจ e-commerce	11
8.3	เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	2
8.4	ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	35
8.5	ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	13
8.6	ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	9
8.7	กลุ่มจัดตั้ง ชมรม สมาคม	10
8.8	ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทย	148
8.9	ผู้ให้บริการโซเชียลมีเดีย	2
9	แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ. ไซเบอร์ฯ	2
	รวม	**1,789**

กรณีของศาลปกครองไทยนั้น แม้ศาลปกครองไม่ได้มีบทบาทโดยตรงในการพิจารณาพิพากษาคดีความผิดทางไซเบอร์หรือระบบคอมพิวเตอร์ก็ตาม แต่ศาลปกครองก็มีอำนาจในการพิจารณาพิพากษาคดีปกครองที่เกี่ยวข้องกับเรื่องดังกล่าวบางประการ เช่น มาตรา 90 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีองค์กรเจ้าหน้าที่ออกคำสั่งทางปกครองใด ๆ ตามพระราชบัญญัติดังกล่าว หรือกรณีมีผู้ฝ่าฝืนกฎหมายที่มีความผิดเป็นโทษทางปกครอง เมื่อคณะกรรมการผู้เชี่ยวชาญได้สั่งลงโทษปรับทางปกครองแก่ผู้ฝ่าฝืน แต่บุคคลดังกล่าวไม่ยอมชำระค่าปรับทางปกครอง หากคณะกรรมการผู้เชี่ยวชาญไม่สามารถดำเนินการบังคับทางปกครองได้ คณะกรรมการผู้เชี่ยวชาญมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ หากศาลปกครองพิจารณาแล้วเห็นว่า คำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย

ศาลปกครองมีอำนาจพิพากษาให้ชำระค่าปรับ ตลอดจนบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้ เป็นต้น

ส่วนการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลของศาลปกครองนั้น ปัจจุบันได้มีประกาศสำนักงานศาลปกครอง เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ลงวันที่ 25 ตุลาคม 2565 เพื่อเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร และใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและเป็นไปตามกฎหมายที่เกี่ยวข้อง ปัจจุบันสำนักงานศาลปกครองได้จัดให้มีระบบการตรวจจับการบุกรุกการโจมตีระบบ ได้แก่ IPS (Intrusion Prevention Systems) WAF (Web App Firewall) และระบบอื่นทำงานร่วมกับ Firewall อุปกรณ์กรองอีเมล (Mail security) อุปกรณ์กรองเว็บ (Web security) อุปกรณ์ตรวจจับการโจมตีจากมัลแวร์ (Antimalware) และโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) มีอุปกรณ์ป้องกันภัยคุกคามที่ไม่รู้จักมาก่อน (zero-day) ที่จะเข้ามาก่อให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของสำนักงานศาลปกครอง หากตรวจพบจะมีการปิดกั้นไม่ให้ลุกลามสู่ระบบเครือข่ายภายในได้ ซึ่งที่ผ่านมายังไม่พบการโจมตีทางไซเบอร์ที่มีความร้ายแรงต่อระบบสารสนเทศของสำนักงานศาลปกครอง

ศาลปกครองไทยได้จัดทำแผนพัฒนาดิจิทัล ระยะ 3 ปี (พ.ศ. 2563 – 2565) เพื่อพัฒนาองค์กรไปสู่การเป็นศาลปกครองอิเล็กทรอนิกส์และศาลปกครองอัจฉริยะ โดยมีการพัฒนาระบบต่าง ๆ ที่สำคัญ เช่น ระบบงานคดีปกครองอิเล็กทรอนิกส์ ระบบห้องพิจารณาอิเล็กทรอนิกส์ ระบบการบริหารจัดการคดี เป็นต้น โดยเฉพาะอย่างยิ่ง ในการดำเนินคดีของประชาชนผ่านระบบดังกล่าว คู่กรณีจำต้องยื่นเอกสารหลักฐานต่าง ๆ ผ่านระบบ ซึ่งส่วนใหญ่จะเป็นเอกสารส่วนบุคคลหรือเป็นพยานหลักฐานในคดีที่สำคัญ หากมีผู้ไม่ประสงค์ดีเจาะเข้าถึงข้อมูลดังกล่าว อาจก่อให้เกิดความเสียหายแก่คู่กรณี รวมถึงความน่าเชื่อถือของศาลปกครองไทยในการใช้ระบบอิเล็กทรอนิกส์ดังกล่าวด้วย เมื่อศาลปกครองได้จัดทำแผนพัฒนาดิจิทัลในฉบับต่อมา โดยนำมาบังคับใช้ระหว่างปี พ.ศ. 2566 – 2570 จึงเล็งเห็นความสำคัญของปัญหาดังกล่าวมากขึ้น โดยในช่วง 3 ปีแรกศาลปกครองได้เน้นพัฒนาเพื่อการนำไปใช้กับการดำเนินคดีได้แท้จริง มีการปรับปรุงข้อกฎหมาย การพัฒนาระบบโปรแกรม การจัดหาอุปกรณ์คอมพิวเตอร์ การอบรมบุคลากร รวมถึงการประชาสัมพันธ์ให้คู่กรณีได้เข้าใจว่าระบบดังกล่าวมีความสะดวกรวดเร็ว และประหยัดทรัพยากรเพียงใด จนมีผู้ใช้บริการมากขึ้นในปัจจุบัน ทั้งนี้ ส่วนหนึ่งก็มาจากการระบาดของโรคโควิด 19 ด้วย

อย่างไรก็ตาม ในช่วงแรกของการใช้ระบบพบว่า มีการโจมตีทางไซเบอร์หลายครั้งในหลายลักษณะตามตารางสถิติด้านล่าง ซึ่งระบบรักษาความปลอดภัยของศาลปกครองสามารถตรวจพบและป้องกันไว้ได้ ดังนี้[4]

[4] ที่มาของข้อมูล – สำนักวิทยาการสารสนเทศ, สำนักงานศาลปกครอง

สถิติภัยคุกคามทางไซเบอร์ในศาลปกครอง

รูปแบบการโจมตีทางไซเบอร์	จำนวนครั้ง
1. Malware	8,932
2. SQL Injection	1,109,082
3. Cross – Site Scripting (XXS)	43,129
4. Denial of Service (DOS) และ Distributed Denial & Service (DDOS)	18,244,719
5. Password Attack	189,517
6. Server – side Request Forgery (SSRF)	1,034
7. Automated Vulnerability Scanning	220,977
8. Suspicious File Extension Access	4,567
9. Hazardous HTTP Request Methods	12,496
10. HTTP : HTTP Login Bruteforce Detected	86,978
11. HTTP : OS Command Execution Unix	126,614

แม้ว่าจะสามารถตรวจพบและป้องกันการโจมตีทางไซเบอร์ลักษณะต่าง ๆ ข้างต้นไว้ได้ แต่ในอนาคตอันใกล้ ศาลปกครองมีนโยบายที่จะนำระบบอิเล็กทรอนิกส์มาใช้อย่างเต็มรูปแบบ รวมถึงการนำปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) มาใช้ในการทำงานด้านต่าง ๆ ของศาลมากขึ้น ศาลปกครองจึงต้องเผชิญกับปัญหาท้าทายใหม่ ๆ จากภัยคุกคามทางไซเบอร์อันมีการพัฒนารูปแบบและความซับซ้อนมากขึ้นทุกวัน

เมื่อสำรวจความท้าทายของศาลปกครองในเรื่องดังกล่าวพบว่า มี 3 ประเด็น ได้แก่

1) ปัญหาอุปกรณ์คอมพิวเตอร์แม่ข่ายและระบบปฏิบัติการที่ศาลปกครองใช้งานอยู่ไม่ทันสมัย ทำให้มีช่องโหว่ที่แฮกเกอร์สามารถโจมตีได้ รวมทั้งไม่มีการทำ Redundant Server ทำให้เมื่อคอมพิวเตอร์แม่ข่ายถูกโจมตีหรือขัดข้อง จะไม่สามารถเปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายสำรองให้ทำงานแทนได้ทันที ต้องนำข้อมูลที่สำรองไว้กู้คืนข้อมูล ซึ่งต้องใช้ระยะเวลาในการดำเนินการนาน

2) ปัญหาระบบสารสนเทศที่ศาลปกครองพัฒนาขึ้นเองโดยใช้เทคโนโลยีเก่า ทำให้มีช่องโหว่ รวมทั้งไม่มีการตรวจสอบช่องโหว่ของระบบก่อนใช้งานจริง

3) ปัญหาบุคลากรของศาลปกครองขาดความรู้ ความเข้าใจ และความตระหนักในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมทั้งไม่มีผู้ดูแลระบบที่มีประสบการณ์และความเชี่ยวชาญ

จากปัญหาความท้าทายข้างต้น ศาลปกครองจึงได้กำหนดยุทธศาสตร์ยกระดับความมั่นคงปลอดภัยทางไซเบอร์ให้มีมาตรฐานไว้ในแผนพัฒนาดิจิทัลฉบับล่าสุด โดยมีเป้าหมายสำคัญสองประการ คือ เพื่อให้ศาลปกครองมีระบบความมั่นคงปลอดภัยดิจิทัลที่ได้มาตรฐานและมีประสิทธิภาพ สามารถป้องกันการโจมตีทางไซเบอร์ได้ รวมทั้งสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการดิจิทัลของศาลทั้งบุคคลภายในและภายนอก

ทั้งนี้ ศาลปกครองได้กำหนดยุทธศาสตร์ของแผนพัฒนาดิจิทัลของศาลปกครอง พ.ศ. 2566 – 2570[5] จำนวน 4 ยุทธศาสตร์ สำคัญ ประกอบด้วย ยุทธศาสตร์ที่ 1 พัฒนาระบบและนวัตกรรมดิจิทัลที่ใช้งานง่าย สะดวก รวดเร็ว ตอบโจทย์ผู้ใช้ ยุทธศาสตร์ที่ 2 บูรณาการเชื่อมโยงข้อมูลทางปกครองเพื่อการบริการและการบริหารจัดการที่ทันสมัย ได้มาตรฐาน ยุทธศาสตร์ที่ 3 ยกระดับความมั่นคงปลอดภัยทางไซเบอร์ให้มีมาตรฐาน และยุทธศาสตร์ที่ 4 พัฒนาบุคลากรและสร้างสรรค์องค์ความรู้เพื่อขับเคลื่อนศาลปกครองอิเล็กทรอนิกส์ที่สมบูรณ์และใช้งานเต็มรูปแบบ

ภายใต้ยุทธศาสตร์ที่ 3 ที่เน้นเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ศาลปกครองได้กำหนดโครงการสำคัญเพื่อสนองต่อยุทธศาสตร์ดังกล่าว จำนวน 3 โครงการ ได้แก่ (1) โครงการพัฒนาโครงสร้างพื้นฐานดิจิทัลอาคารศาลปกครองสูงสุดแห่งใหม่และศูนย์สำรองข้อมูล (Data center) เพื่อบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลของศาลปกครองทั่วทั้งองค์กร (2) โครงการยกระดับความมั่นคงปลอดภัยที่มีมาตรฐานตามแนวทางศูนย์เฝ้าระวังและป้องกันการโจมตีทางไซเบอร์ (SOC) แบบครบวงจร โดยดำเนินงานให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในรูปแบบการเฝ้าระวังและป้องกันการโจมตีทางไซเบอร์ (SOC) แบบครบวงจร (Security Operations Center – SOC) เพื่อการเฝ้าระวังป้องกัน และรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีดิจิทัลให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ตลอด 24 ชั่วโมง (Real time) อันเป็นการยกระดับความปลอดภัยของข้อมูลโดยการเฝ้าระวังและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลเอกสารหลักฐานดิจิทัลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อสร้างความเชื่อมั่นให้กับประชาชน คู่กรณี และหน่วยงานภาครัฐในการใช้บริการศาลปกครองอิเล็กทรอนิกส์ ทั้งนี้ ในปี พ.ศ. 2567 มีกิจกรรมหลัก เช่น การจัดหาและวางระบบคุ้มครองข้อมูลส่วนบุคคลของประชาชนที่เป็นผู้ใช้บริการ (Cookie and Consent Management) การจัดหาอุปกรณ์ป้องกันเครือข่าย (Next Gen Firewall) เป็นต้น โดยกิจกรรมในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะดำเนินการต่อเนื่องไปจนถึงปี พ.ศ. 2570 พร้อมกับการจัดทำรายงานผลการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถพัฒนาระบบฮาร์ดแวร์และซอฟต์แวร์ที่ทันสมัยและทันต่อภัยคุกคามทางไซเบอร์ที่มีการพัฒนาเปลี่ยนแปลงอย่างรวดเร็ว

---

[5] แผนพัฒนาดิจิทัลของศาลปกครอง พ.ศ. 2566 – 2570 มีวัตถุประสงค์ที่สำคัญ คือ สนับสนุนขับเคลื่อนการพัฒนาศาลปกครองให้บรรลุเป้าหมายแผนแม่บทของศาลปกครองระยะ 20 ปี และแผนปฏิบัติราชการสำนักงานศาลปกครอง พ.ศ. 2566 – 2570 โดยใช้แนวทางการพัฒนาตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570 โดยสามารถสรุปสาระสำคัญของแผนพัฒนาดิจิทัลของศาลปกครอง พ.ศ. 2566 – 2570 ดังที่ได้กำหนดวิสัยทัศน์ไว้ว่า “ศาลปกครองอิเล็กทรอนิกส์เพื่อการอำนวยความยุติธรรมทางปกครองที่รวดเร็ว ทันสมัย โปร่งใส และเป็นธรรม”

นอกจากนี้ ศาลปกครองจะมุ่งเน้นแสวงหาความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ โดยเฉพาะการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ที่อาจเกิดขึ้นในอนาคต ทั้งนี้ มีหน่วยงานของรัฐหลายแห่งถูกโจมตีและก่อให้เกิดความเสียหายตามมา เช่น โรงพยาบาล สถานศึกษา เป็นต้น ศาลปกครองจึงได้กำหนดให้สร้างความร่วมมือทางวิชาการกับหน่วยงานรัฐของไทยที่มีความเชี่ยวชาญด้านเทคโนโลยีดิจิทัล เช่น สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. (DGA) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) และสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน) เป็นต้น รวมทั้งจะได้ประสานกับกระทรวงการต่างประเทศในการดำเนินงานผ่านภาคีของปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime) ที่อาจเข้ามาจากต่างประเทศด้วย ซึ่งจะทำให้ศาลปกครองมีความมั่นคงปลอดภัยทางไซเบอร์และสามารถสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการได้อย่างแท้จริงต่อไป

สำหรับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ในประเทศสิงคโปร์นั้น พบว่าในปี พ.ศ. 2566 ประเทศสิงคโปร์ต้องเผชิญกับการโจมตีทางไซเบอร์หลายรูปแบบ ทั้งนี้ ทีมตอบโต้เหตุฉุกเฉินทางคอมพิวเตอร์ของประเทศสิงคโปร์ (Singapore Computer Emergency Response Team หรือ SingCERT) พบว่า มีการหลอกลวงของมิจฉาชีพในลักษณะฟิชชิ่ง (Phishing) อันเป็นการหลอกลวงโดยการสร้างอีเมลปลอม เว็บไซต์ปลอม หรือ SMS ปลอม เป็นต้น เพื่อให้ได้ข้อมูลส่วนบุคคลหรือทำให้บุคคลนั้นสับสนและทำธุรกรรมทางการเงินให้กลุ่มมิจฉาชีพ จำนวน 8,500 กรณี พบการโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) จำนวน 130 กรณี กลุ่มเป้าหมายที่ถูกโจมตี คือ หน่วยธุรกิจขนาดกลางและขนาดย่อม (SMEs) และมีจำนวนโครงสร้างพื้นฐานทางสารสนเทศที่ถูกมัลแวร์ (Malware) เข้าเจาะระบบ (infected) จำนวน 81,500 ระบบ โดยหน่วยงานด้านความมั่นคงทางไซเบอร์ได้ประสานความร่วมมือกับผู้ให้บริการทางด้านอินเทอร์เน็ตที่เกี่ยวข้องเพื่อแก้ไขปัญหาอย่างสม่ำเสมอ นอกจากนี้ ยังพบกรณีของการเข้าไปแก้ไขเว็บไซต์ (Website defacement) แต่จำนวนเว็บไซต์ที่ถูกเข้าไปแก้ไขลดลงจากปีที่ผ่านมา อย่างไรก็ตามการดำเนินการในลักษณะนี้ได้มีการย้ายไปยังแพลตฟอร์มอื่น โดยเฉพาะอย่างยิ่ง สื่อสังคมออนไลน์ (Social media) มีปริมาณที่มากขึ้น

ประเทศสิงคโปร์ได้ประกาศใช้รัฐบัญญัติว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Act, 2018) เพื่อวางกรอบการทำงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ โดยกำหนดให้มีหน่วยงานของรัฐรับผิดชอบ คือ สำนักงานความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Agency : CSA) ซึ่งมีอำนาจตอบสนองต่อภัยคุกคามและเหตุการณ์ทางไซเบอร์ วางกรอบการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดอำนาจหน้าที่ของผู้ที่มีหน้าที่ต้องดำเนินการรับมือต่อการโจมตีทางไซเบอร์ที่สำคัญ รัฐบัญญัติดังกล่าวได้กำหนดให้ระบบคอมพิวเตอร์ถือเป็นโครงสร้างพื้นฐานสำคัญของข้อมูลทางไซเบอร์ (Cyber Information Infrastructure : CII) ซึ่งได้มีการแบ่งประเภทของโครงสร้างพื้นฐานสำคัญของข้อมูลทางไซเบอร์ออกเป็น 11 ภาคส่วน (Sectors) ใน 3 กลุ่ม ได้แก่ ภาคการบริการ (Services) ภาคการสาธารณูปโภค (Utilities) และภาคการขนส่ง (Transport) โดยโครงสร้าง

พื้นฐานสำคัญของข้อมูลทางไซเบอร์ในการบริการภาครัฐจะถูกจัดอยู่ในกลุ่มของการบริการ (Services) สำหรับผู้ที่มีหน้าที่ต้องดำเนินการรับมือต่อการโจมตีทางไซเบอร์นั้น วิทยากรได้กล่าวถึงอำนาจหน้าที่ของผู้ที่เกี่ยวข้อง 3 ลักษณะ ได้แก่ 1) สำนักงานความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Agency : CSA) ซึ่งเป็นหน่วยงานที่ได้รับการมอบหมายให้เป็นผู้บริหารจัดการการรับมือเหตุการณ์ทางไซเบอร์ระดับชาติ มีอำนาจหน้าที่วิจัยและการสร้างความเข้าใจที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ในระดับชาติ และจัดทำข้อเสนอการจัดระดับการเตือนภัยทางไซเบอร์ระดับชาติ (National Cyber-Threat Alert Level : NCTAL) ต่อคณะกรรมการจัดการภัยพิบัติ (Crisis Management Group : CMG) 2) เจ้าหน้าที่ผู้รับผิดชอบในภาคส่วนของโครงสร้างพื้นฐานสำคัญของข้อมูลทางไซเบอร์แต่ละภาคส่วน (Sector lead) ซึ่งทำหน้าที่เป็นผู้บริหารจัดการเหตุการณ์ทางไซเบอร์ที่เกิดขึ้นต่อโครงสร้างพื้นฐานในภาคส่วนนั้น ๆ (Sector Cyber Incident Manager) และ 3) เจ้าของโครงสร้างพื้นฐานสำคัญของข้อมูลทางไซเบอร์ ซึ่งเป็นแนวหน้าที่จะต้องรับมือและตอบสนองต่อเหตุการณ์ทางไซเบอร์ มีหน้าที่เชิงรุกในการป้องกันการโจมตีทางไซเบอร์ เช่น กำหนดให้เจ้าของโครงสร้างพื้นฐานสำคัญของข้อมูลทางไซเบอร์ต้องจัดให้มีแผนดำเนินการเพื่อลดความเสี่ยงทางไซเบอร์ซึ่งจะทำให้สามารถระบุและติดตามภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น

สำหรับการดำเนินการเพื่อรับมือและบรรเทาความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threat Mitigation) ของประเทศสิงคโปร์นั้น รัฐบาลสิงคโปร์ได้ดำเนินการบรรเทาความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น โดยแบ่งประเภทการดำเนินการเป็น 3 เสาหลัก (Pillars) ได้แก่ ด้านยุทธศาสตร์ ด้านวิศวกรรมซอฟต์แวร์ (Engineering) และด้านการปฏิบัติการ (Operation) ในด้านที่มีความโดดเด่นและก้าวหน้าอย่างมาก คือ ด้านวิศวกรรมซอฟต์แวร์ รัฐบาลสิงคโปร์ได้พัฒนาโครงสร้างพื้นฐานในระบบคลาวด์ (Cloud-base infrastructure) ร่วมกับผู้ให้บริการระบบคลาวด์เอกชนชั้นนำ เช่น Google หรือ Amazon Web Service (AWS) เป็นต้น เพื่อให้การบริการและการจัดเก็บข้อมูลของรัฐบาลอยู่บนระบบคลาวด์โดยเรียกว่า Government Commercial Cloud (GCC) ซึ่งรัฐบาลสิงคโปร์ได้อนุญาตให้หน่วยงานของรัฐผู้พัฒนาระบบที่ได้รับอนุญาตและอุปกรณ์เชื่อมต่อต่าง ๆ สามารถเข้าถึงการให้บริการบนระบบ GCC ได้ นอกจากนี้ รัฐบาลสิงคโปร์ยังได้พัฒนาซอฟต์แวร์ที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้นเพื่อช่วยในการพัฒนาแอปพลิเคชันหรือระบบต่าง ๆ ของหน่วยงานภาครัฐให้มีความปลอดภัยตามมาตรฐาน เช่น ระบบ Code Security and Compliance Automation Platform Ecosystem (CodeSCAPE) หรือระบบ Mobile Application Security Hygiene (MASH) เป็นต้น ในส่วนด้านการปฏิบัติการของรัฐบาลสิงคโปร์โดยศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของรัฐบาล Government Cyber Security Operation Center (GCSOC) ได้นำระบบปฏิบัติการเช่นเดียวกันกับที่ใช้ในภาคอุตสาหกรรมด้านเทคโนโลยีมาใช้ปฏิบัติ สำหรับการบริหารจัดการเหตุการณ์ทางไซเบอร์ รัฐบาลสิงคโปร์ได้จัดระดับความรุนแรงของเหตุการณ์ทางไซเบอร์ขึ้นตามธรรมชาติและผลกระทบของเหตุการณ์ออกเป็น 5 ระดับ ตั้งแต่ระดับการโจมตีที่มีความรุนแรงต่ำซึ่งส่งผลเพียงเล็กน้อยต่อหน่วยงานและประชาชนทั่วไป จนถึงระดับการโจมตีที่มีความรุนแรงขั้นสูงสุด (Very severe) ซึ่งส่งผลกระทบต่อความมั่นคงของประเทศ

รวมถึงความน่าเชื่อถือหรือความน่าไว้วางใจของรัฐบาล นอกจากนี้ ยังได้มีการจัดระดับประเภทความรุนแรงในกรณีที่การโจมตีทางไซเบอร์ส่งผลให้เกิดการรั่วไหลทางข้อมูลเป็นการเฉพาะด้วย ทั้งนี้ ในแต่ละระดับความรุนแรงของการโจมตีจะมีเจ้าหน้าที่หรือผู้ที่มีอำนาจในการบริหารจัดการที่แตกต่างกันไป

สำหรับการดำเนินการและแนวปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของศาลยุติธรรมสิงคโปร์ วิทยากรได้กล่าวถึงการดำเนินการต่าง ๆ ซึ่งแบ่งออกเป็น 3 ส่วน ได้แก่ การรักษาความปลอดภัยของแอปพลิเคชันและระบบเครือข่าย (Application and Network security) การจัดการความเปราะบางด้านอุปกรณ์และชุดคำสั่งควบคุมการทำงาน (Hardware and software vulnerabilities) และการดำเนินการเกี่ยวกับบุคลากร (Human Awareness) โดยในการรักษาความปลอดภัยของแอปพลิเคชันและระบบเครือข่าย (Application and Network security) ศาลยุติธรรมสิงคโปร์ได้นำ Web App Firewall (WAF) มาใช้ รวมถึงตรวจสอบผู้เข้าใช้งานอย่างเข้มงวดเพื่อคัดกรองและเฝ้าระวังจากการโจมตีประเภท SQL injection และ Cross-Site Scripting (XSS) การควบคุมการอัปโหลดไฟล์อย่างเข้มงวด และการดำเนินการตรวจสอบระบบ (Audit) ตรวจสอบโค้ดโปรแกรม (Source code review) ประเมินช่องโหว่ (Vulnerability assessments) และทดสอบการเจาะระบบ (Penetration testing) อย่างสม่ำเสมอ โดยการเชิญชวนให้บุคคลทั่วไปแข่งขันการเจาะระบบโดยมีการให้รางวัลกับแฮกเกอร์ (Hacker) ที่สามารถหาจุดอ่อนของระบบได้ อันสะท้อนให้เห็นถึงการมีส่วนร่วมในการป้องกันภัยคุกคามทางไซเบอร์ได้เป็นอย่างดี หรือในการรักษาความปลอดภัยของระบบเครือข่าย (Network security) ศาลยุติธรรมของสิงคโปร์ได้แบ่งเครือข่ายออกเป็นส่วนย่อย ๆ หลายส่วน (Segment networks) เพื่อเพิ่มความปลอดภัยและลดผลกระทบจากการโจมตี โดยเฉพาะเพื่อลดผลกระทบจากการโจมตีในรูปแบบ (Distributed Denial of Service : DDOS) ด้วย ในส่วนของความเปราะบางของอุปกรณ์ (Hardware) และชุดคำสั่งควบคุมการทำงาน (Software) ศาลยุติธรรมสิงคโปร์ได้พยายามในงานลดช่องโหว่ที่เกี่ยวข้องกับอุปกรณ์และชุดคำสั่ง โดยพยายามอัปเดตให้ทันสมัยที่สุดเพื่ออุดช่องโหว่หรือความเปราะบางที่อาจเกิดขึ้น ซึ่งในส่วนของอุปกรณ์ (Hardware) นั้นได้มีการจัดทำแผนเพื่อถ่ายโอนข้อมูลจากอุปกรณ์และระบบปฏิบัติการที่ไม่สามารถอัปเดตได้แล้ว (Unsupported hardware and OS versions) ทั้งนี้ รัฐบาลสิงคโปร์ได้ผลักดันให้มีการนำบริการต่าง ๆ ขึ้นสู่ระบบคลาวด์ (Government on Commercial Clound หรือ GCC) เพื่อลดภาระในการบำรุงรักษาและป้องกันความเปราะบางของอุปกรณ์อันอาจเกิดจากอุปกรณ์ที่ไม่ทันสมัย นอกจากนี้ รัฐบาลสิงคโปร์ยังได้เน้นย้ำถึงความสำคัญของบุคลากรในองค์กรต่อการป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์ โดยไม่ใช่เพียงเป็นหน้าที่ของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเท่านั้น แต่เกี่ยวข้องกับผู้ที่ต้องใช้ระบบทุกคน หากบุคคลใดบุคคลหนึ่งประมาทเลินเล่อเพียงเล็กน้อยก็อาจเป็นจุดอ่อนที่ทำให้ระบบความปลอดภัยทางไซเบอร์ทั้งระบบตกอยู่ในอันตรายได้ การให้ความรู้และการเสริมสร้างความตระหนักรู้ (Education and awareness) แก่บุคลากรในองค์กรจึงเป็นสิ่งสำคัญอย่างมากและควรดำเนินการอย่างต่อเนื่อง

ในช่วงของการถามตอบนั้น ผู้เข้าร่วมรับฟังมีคำถามในหลากหลายประเด็น ทั้งในส่วนของสถานการณ์ด้านการโจมตีทางไซเบอร์ของสิงคโปร์และนโยบายการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของสิงคโปร์ เช่น ศาลยุติธรรมสิงคโปร์เคยถูกโจมตีทางไซเบอร์โดยที่ผู้โจมตีอยู่ต่างประเทศบ้างหรือไม่ ซึ่งวิทยากรได้ตอบว่า ศาลยุติธรรมสิงคโปร์ใช้บริการของศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของรัฐบาล (Government Cyber Security Operation Center (GCSOC)) ในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ข้อมูลในส่วนนี้จึงจะถูกจัดเก็บที่หน่วยงานดังกล่าว ทั้งนี้ การโจมตีจากต่างประเทศเป็นสิ่งที่พบได้ทั่วไป อย่างไรก็ตาม ยังไม่พบการโจมตีที่มีความร้ายแรงและสร้างปัญหาให้แก่ระบบการทำงานของศาล ส่วนคำถามที่ว่า ศาลยุติธรรมสิงคโปร์แก้ไขปัญหาเพื่อลดภาระงบประมาณที่สูงในการป้องกันภัยคุกคามทางไซเบอร์อย่างไร วิทยากรได้ตอบว่า รัฐบาลสิงคโปร์ได้มีความพยายามที่จะผลักดันให้การบริการของรัฐบาลจัดทำอยู่บนระบบคลาวด์ (GCC) เพื่อลดปัญหาในการบริหารจัดการอุปกรณ์ และให้การดำเนินการดังกล่าวเป็นหน้าที่ของผู้ให้บริการระบบคลาวด์ซึ่งเป็นเอกชนชั้นนำแทน ส่วนการบริหารจัดการบุคลากรนั้น ต้องยอมรับว่าการสรรหาบุคลากรในการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นเป็นสิ่งที่มีข้อจำกัดมาก ทั้งในแง่ของจำนวนบุคลากรและค่าจ้างที่ค่อนข้างสูง ดังนั้น จึงจำเป็นที่ต้องจำแนกให้ได้ว่างานหรือทักษะประเภทใดที่สามารถบริหารจัดการได้ด้วยเจ้าหน้าที่ของศาลเอง หรืออาจขอความช่วยเหลือจากหน่วยงานส่วนกลาง เพื่อจำกัดจำนวนบุคลากรที่ต้องใช้ให้มีเท่าที่จำเป็น เมื่อมีการใช้ศักยภาพจากหน่วยงานส่วนกลางเต็มศักยภาพแล้วจึงค่อยประเมินประเภทของงานหรือทักษะที่ตรงกับความต้องการของงานเฉพาะด้านของหน่วยงานต่าง ๆ และประเมินว่างานดังกล่าวสามารถให้บุคคลภายนอกจัดทำ (Outsourced) ได้หรือไม่ เนื่องจากการที่หน่วยงานแต่ละหน่วยงานจะต้องไปพัฒนาบุคลากรของตนเองในการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นอาจเป็นการยากและมีค่าใช้จ่ายที่มากเกินไป และคำถามที่ว่า ปัจจุบันศาลปกครองไทยได้มีการจัดทำแผนการรับมือทางไซเบอร์แล้ว โดยได้มีการกำหนดหน้าที่และขั้นตอนการดำเนินงานในส่วนที่เกี่ยวข้องเสนอต่อเลขาธิการสำนักงานศาลปกครองแล้ว การจัดตั้งหน่วยการตอบโต้ต่อสถานการณ์ทางไซเบอร์ (Incident response team : IRT) และศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation center) ในส่วนของศาลยุติธรรมสิงคโปร์นั้น มีการดำเนินการหรือไม่ อย่างไร ซึ่งวิทยากรได้กล่าวว่า ศาลยุติธรรมสิงคโปร์ยังไม่มีการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของตนเอง โดยยังคงพึ่งพาศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของรัฐบาล GCSOC เนื่องจากไม่มีทรัพยากรบุคคลที่จะต้องดำเนินการเฝ้าระวังตลอดเวลา ในการนี้ จึงต้องมีการจัดทำระบบในการจัดส่งข้อมูลด้านความปลอดภัยไปยัง GCSOC แบบทันทีทันใด (Real-time) เพื่อให้ GCSOC สามารถตรวจจับ ประเมินการโจมตีทางระบบ และแจ้งเตือนไปยังสำนักงานเพื่อจะได้รับมือและดำเนินการสอบสวนเหตุการณ์ได้อย่างทันท่วงที