ความมั่นคงปลอดภัยทางไซเบอร์

CYBER SECURITY

ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

(Cyber Security)

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือและลดความเสี่ยงจาก***ภัยคุกคามทางไซเบอร์***ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐความมั่นคงทางเศรษฐกิจความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

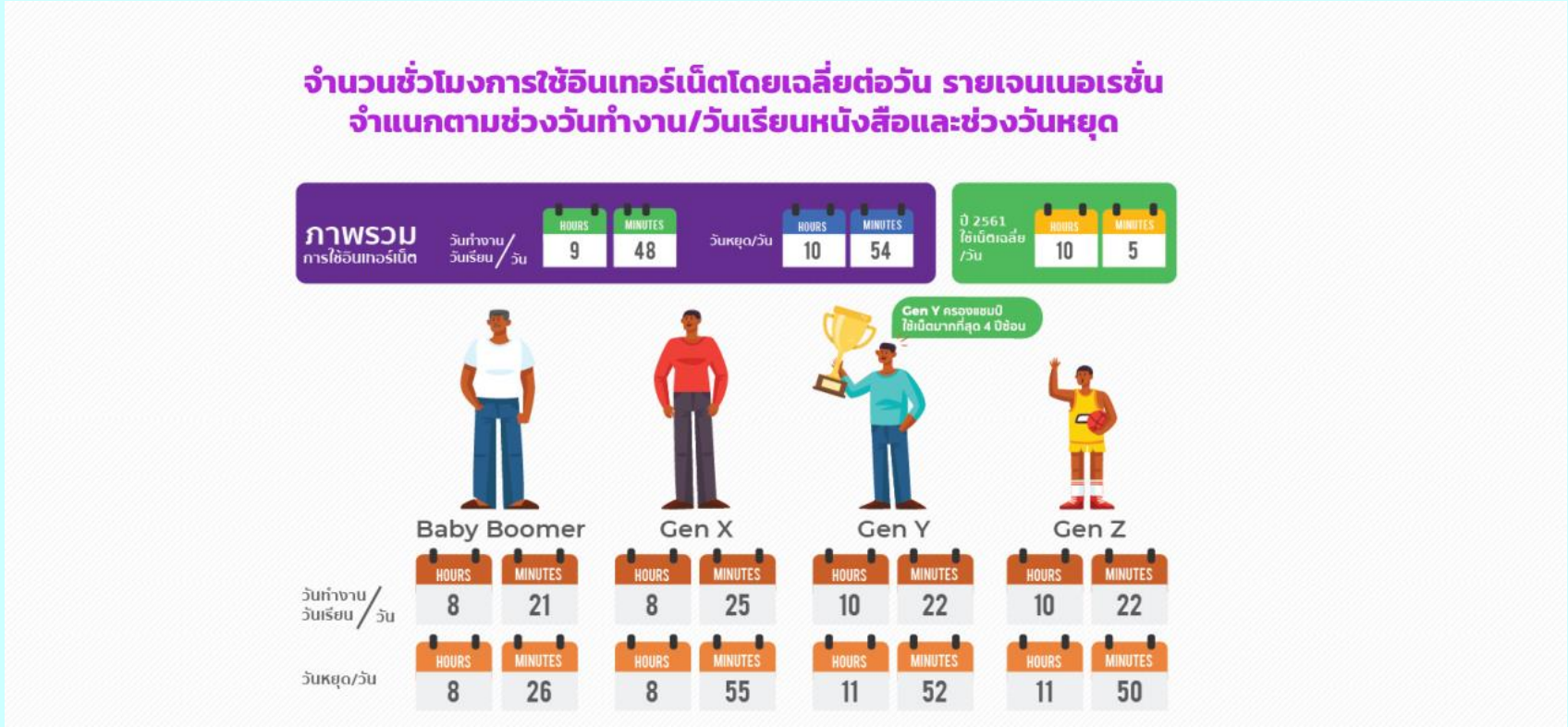
(Cyber Security)

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) มีความสำคัญอย่างไร

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสารจึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กับสำนักงาน กปร.



ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กับสำนักงาน กปร.

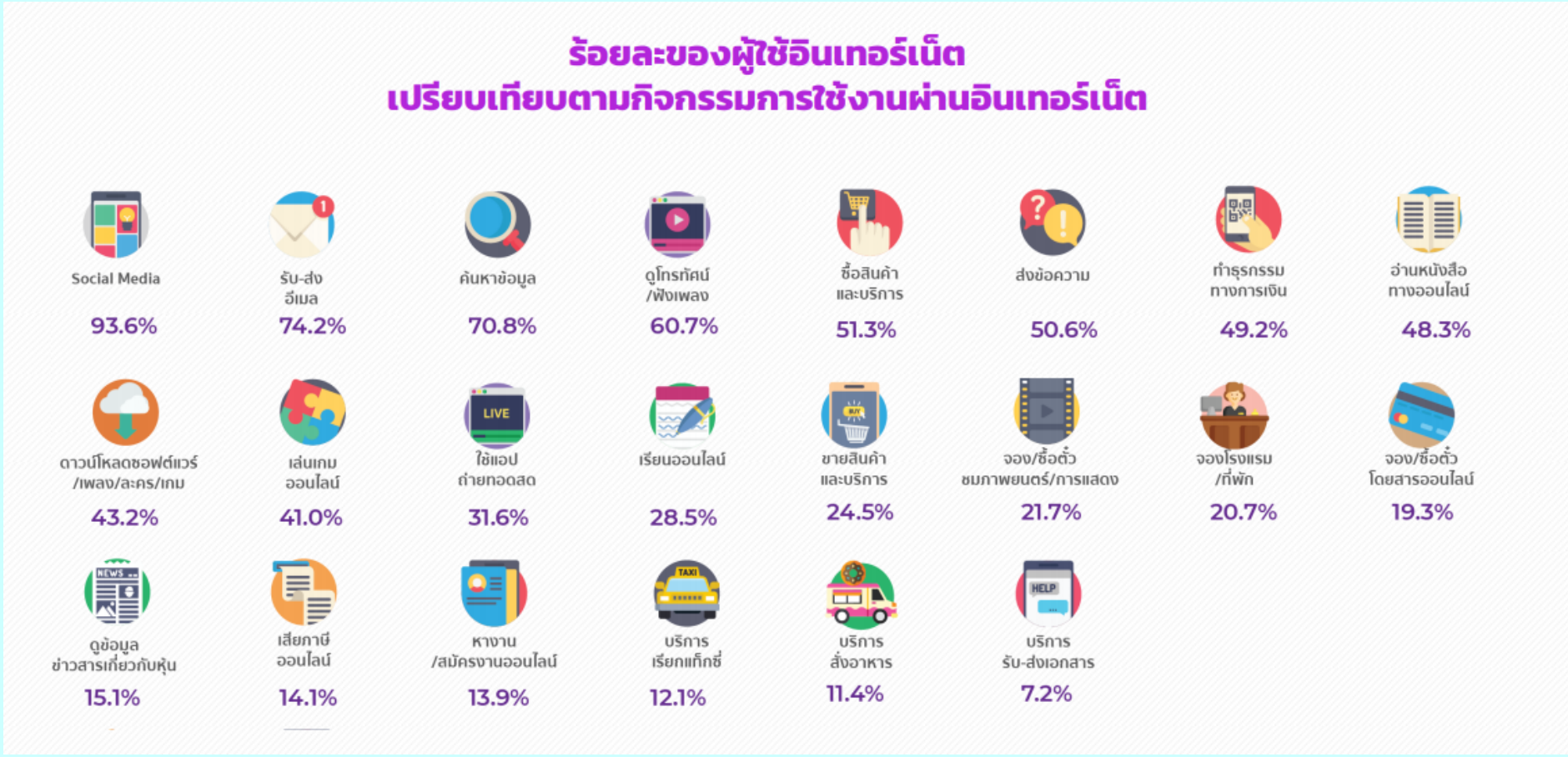
ร้อยละของผู้ใช้อินเทอร์เน็ต
จำแนกตามสถานที่ที่ใช้อินเทอร์เน็ต ปี 2560 – 2561






	บ้าน/ที่พักอาศัย	ที่ทำงาน	ระหว่างเดินทาง	ที่สาธารณะ	สถานศึกษา	อินเทอร์เน็ตคาเฟ่
ปี 2561	91.5% ▲	52.2% ▼	33.5% ▲	21.0% ▲	20.7% ▲	1.1% ▼
ปี 2560	85.6%	52.4%	24.1%	18.8%	17.5%	2.3%

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กับสำนักงาน กปร.



ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กับสำนักงาน กปร.

อุปกรณ์ป้องกันระบบเครือข่าย

1. Firewall ยี่ห้อ Juniper รุ่น SRX1500 ทำหน้าที่เป็นตัวกรองข้อมูลสื่อสาร โดยการกำหนดกฎระเบียบมาบังคับใช้ โดยเฉพาะเรื่องของการดูแลระบบเครือข่าย และความผิดพลาดของการปรับแต่งอาจส่งผลทำให้ไฟล์วอลล์มีช่องโหว่ และนำไปสู่สาเหตุของการโจรกรรมข้อมูลทางคอมพิวเตอร์ได้

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กับสำนักงาน กปร.

อุปกรณ์ป้องกันระบบเครือข่าย

2. Intrusion Prevention System(IPS) ยี่ห้อ Check Point รุ่น 4000 Series สามารถทำการจับรูปแบบของข้อมูลมาทำการวิเคราะห์ เพื่อดูพฤติกรรม การทำงานว่าเป็นความเสี่ยงที่ส่งผลกระทบต่อระบบงานหรือไม่ เช่น Packet ที่ทำงานแบบเดิม ๆ และบ่อยมาก ๆ และมีผลต่อเครือข่ายหรือระบบงาน
เมื่อมีการติดตั้งระบบ IDS/IPS ในองค์กร จะมีผลให้ระบบงานมีความปลอดภัยจากการ บุกรุกทั้งบุคคลภายในและจากเครือข่ายภายนอกได้มากขึ้น และส่งผลให้เครือข่ายภายในองค์กร มีประสิทธิภาพทางด้านความปลอดภัยมากยิ่งขึ้น

ภัยคุกคามทางไซเบอร์กับสำนักงาน กปร.

ภัยคุกคามทางไซเบอร์ที่พบในระบบเครือข่ายของสำนักงาน กปร. มีดังนี้

1. DDoS หรือเรียกอีกอย่างหนึ่งว่า Distributed Denial of Service (DDoS) คือ การโจมตีเครื่องคอมพิวเตอร์เป้าหมายหรือระบบเป้าหมายบนอินเทอร์เน็ตของแฮกเกอร์ เพื่อทำให้ระบบเป้าหมายไม่มีการตอบสนองต่อการร้องขอหรือหยุดให้บริการ (Denial-of-Service) โดยลักษณะของการโจมตีจะมีอยู่หลากหลายรูปแบบได้แก่

- การโจมตีแบบ Ping of Death
- การโจมตีแบบ UDP Flood
- การโจมตีแบบ TearDrop

2. Ransomware หรือ มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ (Malware) ที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ คือ ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้อื่นแต่อย่างใด แต่จะเข้ารหัสหรือล็อคไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วีดีโอ ผู้ใช้งานจะไม่สามารถเปิดหรือเข้าถึงไฟล์เหล่านั้นได้ ดังนั้นผู้ใช้จะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” เพื่อปลดล็อคกู้ข้อมูลคืนมา