“บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก”

“NIST’s Framework for Improving Critical Infrastructure Cybersecurity”

... โอกาส ภัยคุกคาม และความเสี่ยงที่ผู้บริหารองค์กรต้องตระหนัก ...

อาจารย์ปริญญา หอมเอนก and ACIS Research LAB

ในขณะที่อินเทอร์เน็ตกำลังเป็นเครื่องมือสำคัญสำหรับการพัฒนาความเจริญเติบโตทางเศรษฐกิจของทุกประเทศทั่วโลก และขณะเดียวกันอินเทอร์เน็ตกลายเป็นเวทีสำหรับการแลกเปลี่ยนความคิดเห็นของประชาชนในหลายประเทศทั่วโลก จากรายงานของ World Economic Forum แสดงให้เห็นว่าทั่วโลกกำลังวิตกกังวลกับภัยคุกคามด้านไซเบอร์เป็นอย่างมาก โดยภัยคุกคามด้านไซเบอร์ถูกจัดให้อยู่ในอันดับที่ ๔ ใน ๑๐ Trends ของโลก (รูปที่ ๑ อันดับแนวโน้มภัยคุกคามไซเบอร์ทั่วโลกประจำปี ๒๐๑๔ - Global Agenda 2014, World Economic Forum) ประกอบกับรายงานผลการศึกษาของสถาบัน BCI (The Business Continuity Institute) ซึ่งเป็นสถาบันอันดับหนึ่งของโลกด้านการบริหารความต่อเนื่องทางธุรกิจ ยังแสดงให้เห็นว่า Cyber Attack เป็นประเด็นอันดับต้น ๆ ที่องค์กรให้ความสนใจมากที่สุด (รูปที่ ๒ แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยที่องค์กรทั่วโลกตระหนัก - Threat Horizon Scan 2014, BCI)

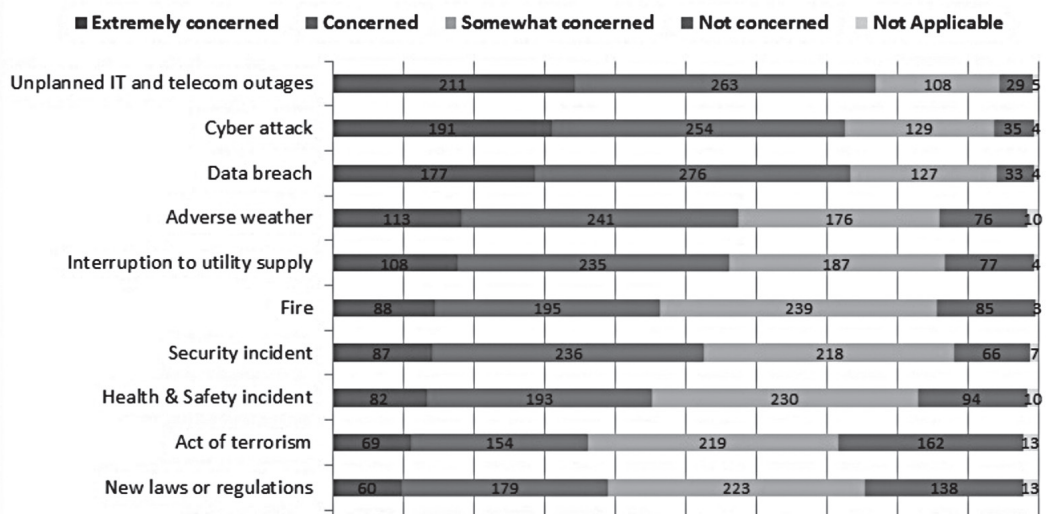
เนื่องจากในปัจจุบันและอนาคต องค์กรหลายแห่งกำลังถูกคุกคามอย่างต่อเนื่องจากการโจมตีทางไซเบอร์ (Cyber Attack) ซึ่งหลายคนอาจมองว่าเป็นภัยที่ไกลตัวหรือดูเหมือนเป็นเรื่องราวในแนวนวนิยายไซไฟ แต่ถ้าหากเราได้มีโอกาสเห็นรายงานการโจมตีสดๆ จากเว็บไซต์ “Digital Attack Map” ซึ่งเป็นเว็บไซต์ที่มีการรวบรวมข้อมูลการโจมตีและแสดงผล Top Daily DDoS Attacks แบบ Real-time (รูปที่ ๓ ภาพรวมการโจมตีทางไซเบอร์ที่มีอย่างต่อเนื่องทั่วโลก และรูปที่ ๔ ภาพรวมการโจมตีทางไซเบอร์ของประเทศไทย ที่มีการโจมตีหนักในช่วงเดือนธันวาคม พ.ศ. ๒๕๕๖) และ “Akamai” ซึ่งเป็นเว็บไซต์ที่รวบรวมข้อมูลความหนาแน่นของระดับการโจมตีทางไซเบอร์ (รูปที่ ๕ ภาพรวมความหนาแน่นของระดับการโจมตีทางไซเบอร์กระจายทั่วโลก และรูปที่ ๖ ภาพรวมความหนาแน่นของระดับการโจมตีทางไซเบอร์ของประเทศไทย) ก็จะทำให้เข้าใจได้ว่าการโจมตีด้านไซเบอร์นั้นได้เกิดขึ้นจริงอยู่ตลอดเวลาทั่วโลก เพียงแต่เราจะมองเห็น รับรู้ หรือไม่รับรู้เท่านั้น

Top trends for 2014, ranked by global significance

1.	Rising societal tensions in the Middle East and North Africa	4.07
2.	Widening income disparities	4.02
3.	Persistent structural unemployment	3.97
4.	Intensifying cyber threats	3.93
5.	Inaction on climate change	3.81
6.	The diminishing confidence in economic policies	3.79
7.	A lack of values in leadership	3.76
8.	The expanding middle class in Asia	3.75
9.	The growing importance of megacities	3.48
10.	The rapid spread of misinformation online	3.35

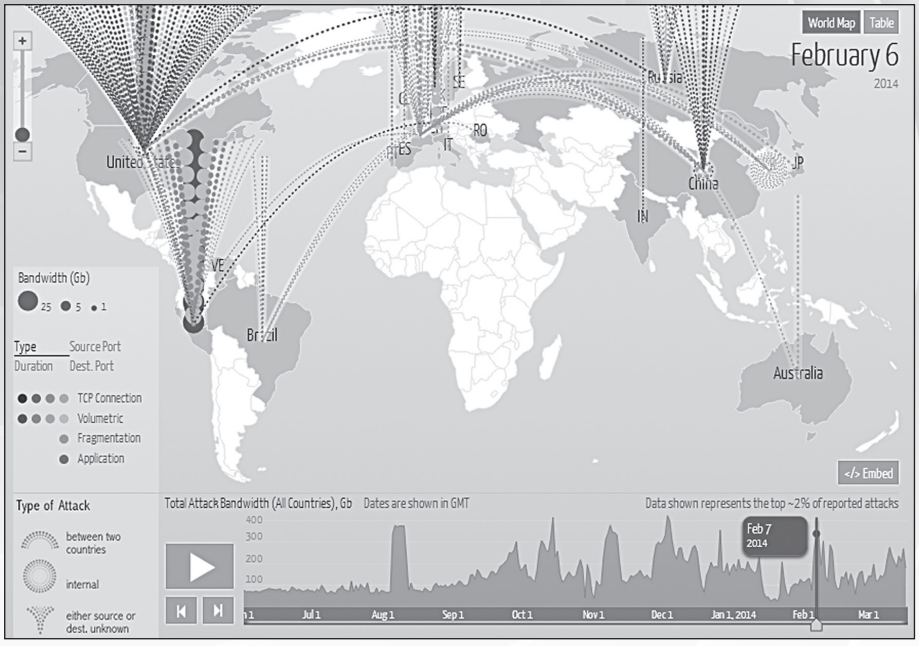
รูปที่ ๑ อันดับแนวโน้มภัยคุกคามไซเบอร์ทั่วโลกประจำปี ๒๐๑๔ จากงานวิจัยสถิติของการประชุมเศรษฐกิจโลก

Source: Global Agenda 2014, World Economic Forum



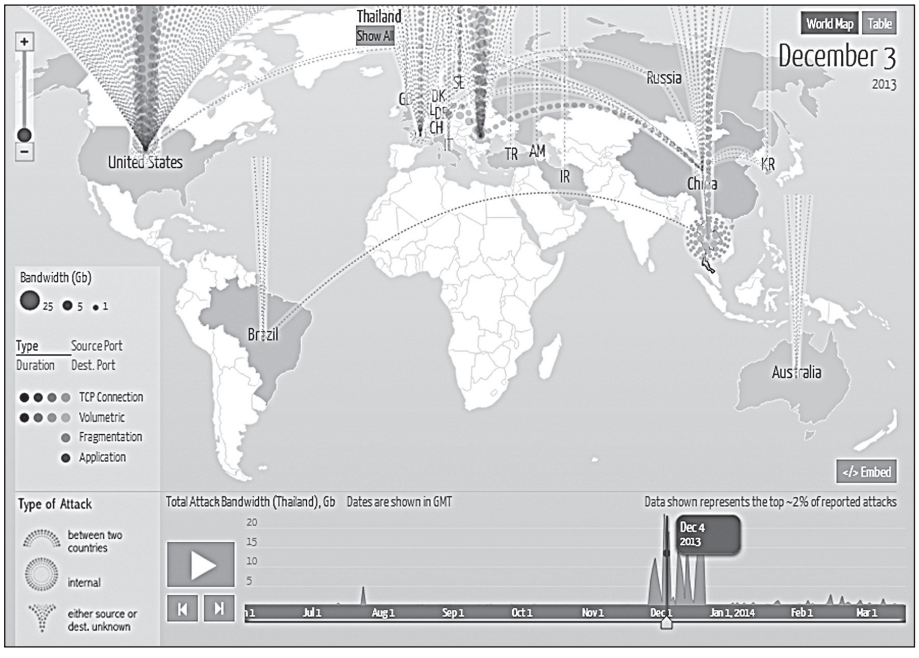
รูปที่ ๒ แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยที่องค์กรทั่วโลกตระหนัก ปี ๒๐๑๔ งานวิจัยโดยสถาบัน BCI

Source: Threat Horizon Scan 2014, The BCI



รูปที่ ๓ ภาพรวมการโจมตีทางไซเบอร์ที่มีอย่างต่อเนื่องทั่วโลก

Source: Digital Attack Map Real-time Data - Top Daily DDoS Attacks Worldwide (All Countries)
http://www.digitalattackmap.com/#anim=1&color=o&country=TH&time=16051&view=map



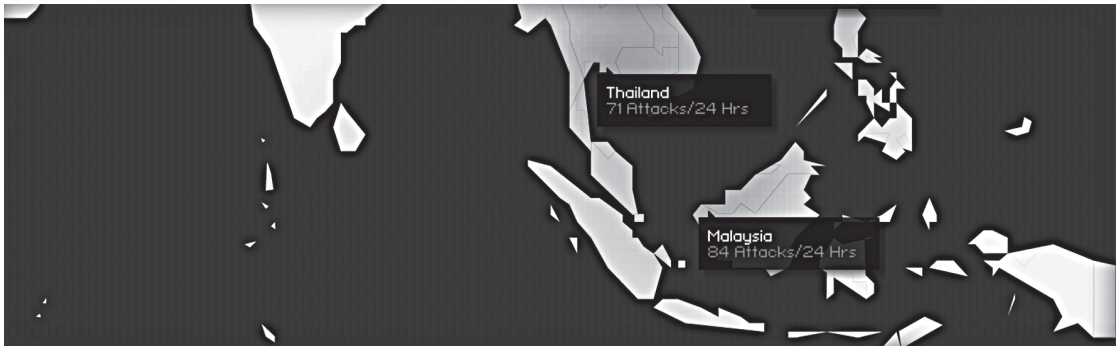
รูปที่ ๔ ภาพรวมการโจมตีทางไซเบอร์ของประเทศไทย ที่มีการโจมตีหนักในช่วงเดือนธันวาคม ๒๕๕๖

Source: Digital Attack Map Real-time Data - Top Daily DDoS Attacks Worldwide (Thailand)
http://www.digitalattackmap.com/#anim=1&color=o&country=TH&time=16051&view=map



รูปที่ ๕ ภาพรวมความหนาแน่นของระดับการโจมตีทางไซเบอร์กระจายทั่วโลก

Source: Akamai Real-time Web Monitor - Attack Traffic Overview (Global)
http://www.akamai.com/html/technology/dataviz1.html

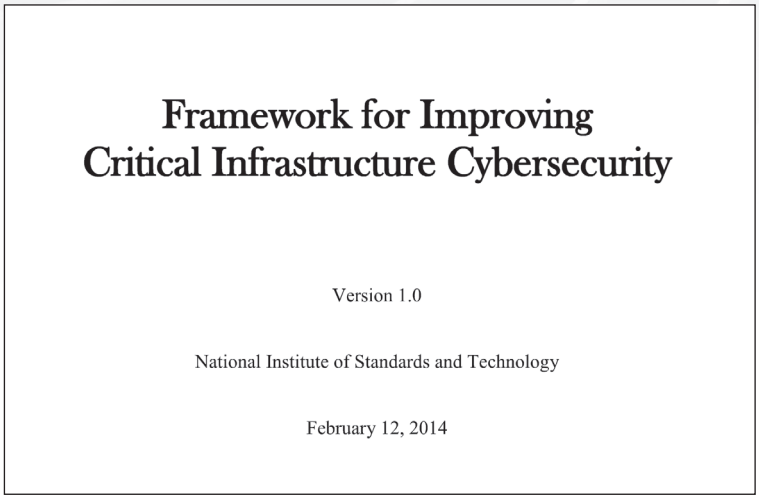


รูปที่ ๖ ภาพรวมความหนาแน่นของระดับการโจมตีทางไซเบอร์ของประเทศไทย

Source: Akamai Real-time Web Monitor - Attack Traffic Overview (Thailand)
http://www.akamai.com/html/technology/dataviz1.html

เนื่องจากการแก้ปัญหาด้านภัยคุกคามทางไซเบอร์อย่างจริงจังต้องการแนวทางอย่างเป็นระบบเพื่อการบริหารจัดการความเสี่ยงดังกล่าวได้อย่างมีประสิทธิภาพและประสิทธิผล ทางรัฐบาลของประเทศสหรัฐอเมริกาภายใต้การบริหารของประธานาธิบดีบารัค โอบามา ได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และเทคโนโลยี เพื่อบริหารความเสี่ยงไซเบอร์ ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม

เอกสารกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์นี้ มีที่มาจากการออกเอกสารฉบับหนึ่งที่เรียกว่า “Cybersecurity Executive Order 13686 -- Improving Critical Infrastructure Cybersecurity” โดยประธานาธิบดีบารัค โอบามา เมื่อวันที่ ๑๕ กุมภาพันธ์ พ.ศ. ๒๕๕๖ เป็นการกำหนดนโยบายเกี่ยวกับความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) มีการกำหนดนโยบายในการแชร์ข้อมูล (Information Sharing) ระหว่างหน่วยงานของรัฐและเอกชน ซึ่งต่อมาได้มอบหมายให้ NIST จัดสัมมนา “Voluntary Cybersecurity Framework” เพื่อระดมความคิดจากทั้งหน่วยงานรัฐและเอกชนต่าง ๆ ซึ่งก่อให้เกิดความสำเร็จอย่างสัมฤทธิผลจากการให้ความร่วมมืออย่างเต็มที่จากความเห็นของทุกภาคส่วน รวมกับกรอบการดำเนินงานตามมาตรฐานและแนวปฏิบัติที่ดี เพื่อปรับปรุงให้เป็น “National Cybersecurity Framework” ฉบับสมบูรณ์ โดยได้นำมาจัดทำเป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ เรียกว่า “Framework for Improving Critical Infrastructure Cybersecurity” (รูปที่ ๗ มาตรฐานกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ, NIST)


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

รูปที่ ๗ มาตรฐานกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ

Source: “Framework for Improving Critical Infrastructure Cybersecurity”, NIST, 12-Feb-2014

NIST ได้ทำการออกเวอร์ชั่นล่าสุดของกรอบการดำเนินงานดังกล่าว เมื่อวันที่ ๑๒ กุมภาพันธ์ พ.ศ. ๒๕๕๗ เป็นกรอบการดำเนินงานที่ประกอบด้วยสามองค์ประกอบหลักที่เรียกว่า “Framework Core”, “Framework implementation Tiers” และ “Framework Proles” เพื่อกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ในการจัดการระบบของหน่วยงานในอุตสาหกรรมที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ ครอบคลุม ๑๖ กลุ่มสำคัญ (http://www.dhs.gov/critical-infrastructure-sectors) ประกอบด้วย

๑) Chemical Sector

๒) Commercial Facilities Sector

๓) Communications Sector
๔) Critical Manufacturing Sector
๕) Dams Sector
๖) Defense Industrial Base Sector
๗) Emergency Services Sector
๘) Energy Sector
๙) Financial Services Sector
๑๐) Food and Agriculture Sector
๑๑) Government Facilities Sector
๑๒) Healthcare and Public Health Sector
๑๓) Information Technology Sector
๑๔) Nuclear Reactors, Materials, and Waste Sector
๑๕) Transportation Systems Sector
๑๖) Water and Wastewater Systems Sector

โครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ (Framework Core)

องค์ประกอบของ Framework Core เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย

- หน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม ในเอกสารนี้ จำแนกเป็น ๕ functions (IPDRR: Identify, Protect, Detect, Respond, Recover)
- กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง
- กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ
- ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

องค์ประกอบ Framework Core Functions แบ่งย่อยออกเป็นกรอบงานหลัก ๕ functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่

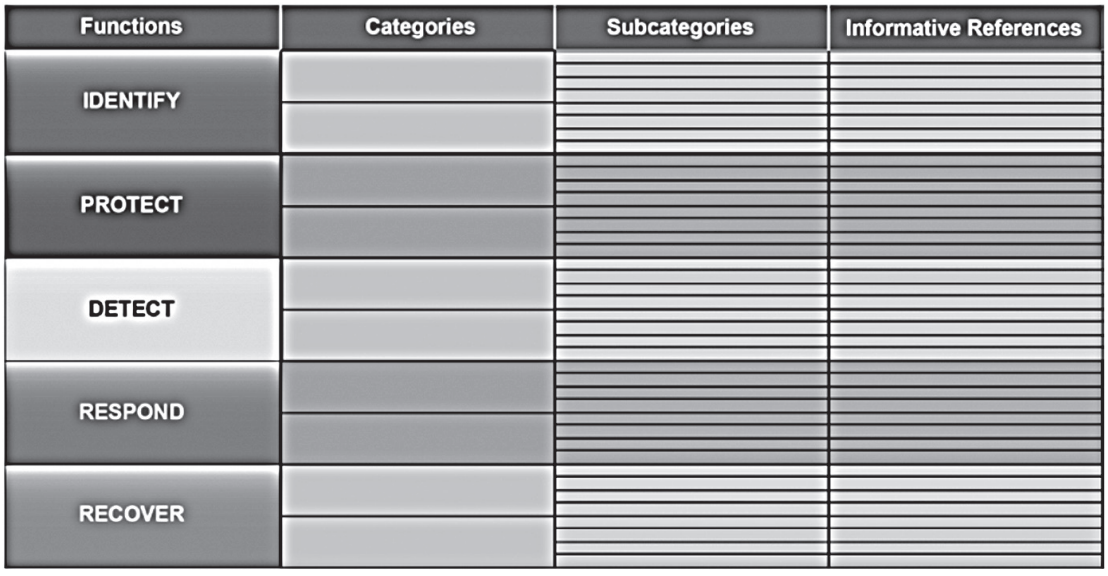
- การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ
- การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

• การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

• การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

• การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

เมื่อองค์กรสามารถใช้ทั้ง ๕ functions ได้อย่างเหมาะสม โดยการกำหนดผลลัพธ์ที่ต้องการ และกรอบปฏิบัติที่อ้างอิงสำหรับการดำเนินงานเพื่อบรรลุตามวัตถุประสงค์ของแต่ละอุตสาหกรรม/โครงสร้างพื้นฐาน จะช่วยให้องค์กรเข้าใจ และจัดทำโครงงานและระบบด้าน Cybersecurity ได้อย่างมีประสิทธิภาพมากขึ้น (รูปที่ ๘ โครงสร้างองค์ประกอบของกรอบงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ “Framework Core Structure”) และรายละเอียดการจำแนกกลุ่มงาน (ตารางที่ ๑ รายละเอียดกลุ่มงานจำแนกตามกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ - Function and Category Unique Identifiers)



รูปที่ ๘ โครงสร้างองค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์

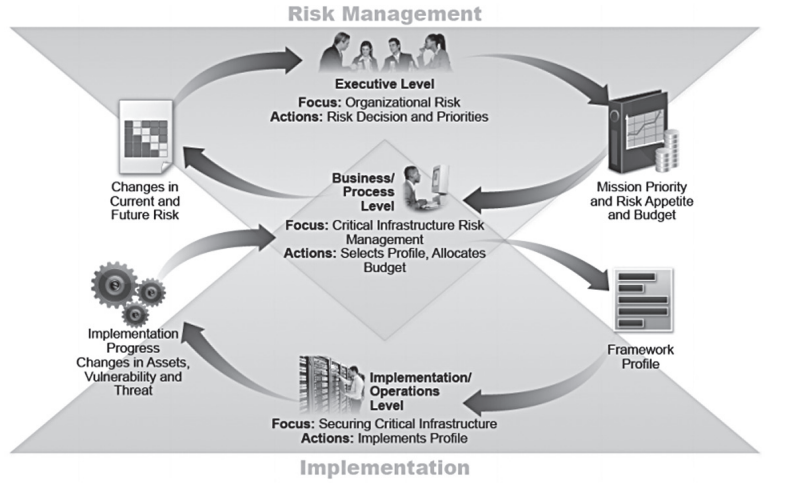
Source: “Framework core structure”, Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014

ตารางที่ ๑ รายละเอียดกลุ่มงานจำแนกตามกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์

(Function and Category Unique Identifiers)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify ระบุ	ID.AM	Asset Management การบริหารจัดการทรัพย์สิน
		ID.BE	Business Environment สภาพแวดล้อมทางธุรกิจ
		ID.GV	Governance การกำกับดูแล (ธรรมาภิบาล)
		ID.RA	Risk Assessment การประเมินความเสี่ยง
		ID.RM	Risk Management Strategy กลยุทธ์การบริหารความเสี่ยง
PR	Protect ป้องกัน	PR.AC	Access Control การควบคุมการเข้าถึง
		PR.AT	Awareness and Training การสร้างความตระหนักและการฝึกอบรม
		PR.DS	Data Security การรักษาความปลอดภัยของข้อมูล
		PR.IP	Information Protection Processes and Procedures กระบวนการและวิธีการในการป้องกันข้อมูล
		PR.MA	Maintenance การบำรุงรักษา
		PR.PT	Protective Technology เทคโนโลยีในการป้องกัน
DE	Detect ตรวจจับ	DE.AE	Anomalies and Events ความผิดปกติและเหตุการณ์
		DE.CM	Security Continuous Monitoring การเฝ้าระวังความมั่นคงปลอดภัยอย่างต่อเนื่อง
		DE.DP	Detection Processes กระบวนการตรวจจับ
RS	Respond ตอบสนอง	RS.RP	Response Planning การวางแผนการตอบสนอง
		RS.CO	Communications การสื่อสาร
		RS.AN	Analysis การวิเคราะห์
		RS.MI	Mitigation การลดผลกระทบ
		RS.IM	Improvements การปรับปรุงการตอบสนอง
RC	Recover คืนสภาพ	RC.RP	Recovery Planning แผนการคืนสภาพ
		RC.IM	Improvements การปรับปรุงการคืนสภาพ
		RC.CO	Communications การสื่อสาร

วิธีการนำ Cybersecurity Framework ดังกล่าวนี้ มาใช้ในองค์กร ให้พิจารณาถึงการไหลเวียนของข้อมูลและการตัดสินใจระดับต่าง ๆ ในองค์กร ได้แก่ ระดับบริหาร ระดับกระบวนการ/ธุรกิจ และระดับปฏิบัติการ โดยจำเป็นต้องมีการประสานงานกับส่วนงานต่างๆ ที่เกี่ยวข้องอย่างเหมาะสม ดังตัวอย่างภาพอธิบายตามแนวคิด (รูปที่ ๙ แนวคิดการไหลเวียนของข้อมูลและการตัดสินใจในองค์กรตามกรอบ Cybersecurity Framework) กล่าวคือ ระดับบริหาร (Executive level) แสดงถึงการส่งต่อข้อมูลที่เกี่ยวข้องกับการตัดสินใจในส่วนต่าง ๆ ในองค์กร โดยที่ระดับบริหาร (Executive level) จะต้องทำการสื่อสารเกี่ยวกับเป้าหมายที่สำคัญต่างๆ ขององค์กร ทรัพยากรที่มีและที่นำมาใช้ได้ ตลอดจนความเสี่ยงที่กระทบองค์กรในระดับกระบวนการ ระดับกระบวนการ (business/process level) ก็จะนำข้อมูลจากระดับผู้บริหาร เพื่อใช้ในกระบวนการจัดการความเสี่ยง และประสานงานกับระดับปฏิบัติการเพื่อจะสื่อสารความต้องการขององค์กร และทำการปฏิบัติการได้อย่างเหมาะสม ระดับปฏิบัติการ (Implementation/Operation level) จะต้องสื่อสารข้อมูลด้านความคืบหน้าของการปฏิบัติการ กลับไปยังฝ่ายกระบวนการเพื่อจะประเมินผลกระทบ ซึ่งจะถูกรายงานกลับไปยังระดับบริหารเพื่อให้เห็นภาพรวมของการบริหารความเสี่ยง และฝ่ายปฏิบัติการก็จะนำข้อมูลดังกล่าวไปใช้เพื่อสร้างความตระหนักเกี่ยวกับผลกระทบของความเสี่ยงที่มีต่อองค์กร



รูปที่ ๙ แนวคิดการไหลของข้อมูลและการตัดสินใจในองค์กรตามกรอบ Cybersecurity Framework

Source: "Notional Information and Decision Flows within an organization", Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014

กรอบการดำเนินงาน Cybersecurity Framework นี้ สามารถนำมาใช้ในองค์กรทั่วไปที่ไม่ได้จัดอยู่ในหน่วยงานโครงสร้างพื้นฐานสำคัญ และโดยสามารถนำมาประยุกต์ใช้โดยไม่จำเป็นต้องมาใช้แทนกระบวนการบริหารความเสี่ยงที่มีอยู่ แต่ให้เป็นส่วนหนึ่งหรือใช้ร่วมกับกระบวนการที่องค์กรมีอยู่ เพื่อใช้ในการระบุ ประเมิน และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ กรอบการดำเนินงาน Cybersecurity Framework มีรูปแบบวิธีการและแนวคิดเพื่อการนำมาใช้ในลักษณะที่ไม่แตกต่างจากแนวทางการดำเนินงานตามแนวคิด GRC (การกำกับดูแลที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ) ดังนี้

(๑) ทบทวนแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

(๒) จัดทำหรือปรับปรุงแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีลำดับขั้นตอนสอดคล้องตาม

กระบวนการบริหารความเสี่ยงได้ การจัดลำดับวัตถุประสงค์และขอบเขตที่จะดำเนินการ การระบุปัจจัยเสี่ยง การจัดทำสถานภาพปัจจุบัน (ตามกลุ่มงานและกลุ่มงานย่อยของผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์) การประเมินความเสี่ยง การจัดทำสภานภาพเป้าหมาย การประเมินวิเคราะห์ และการดำเนินแผนงาน

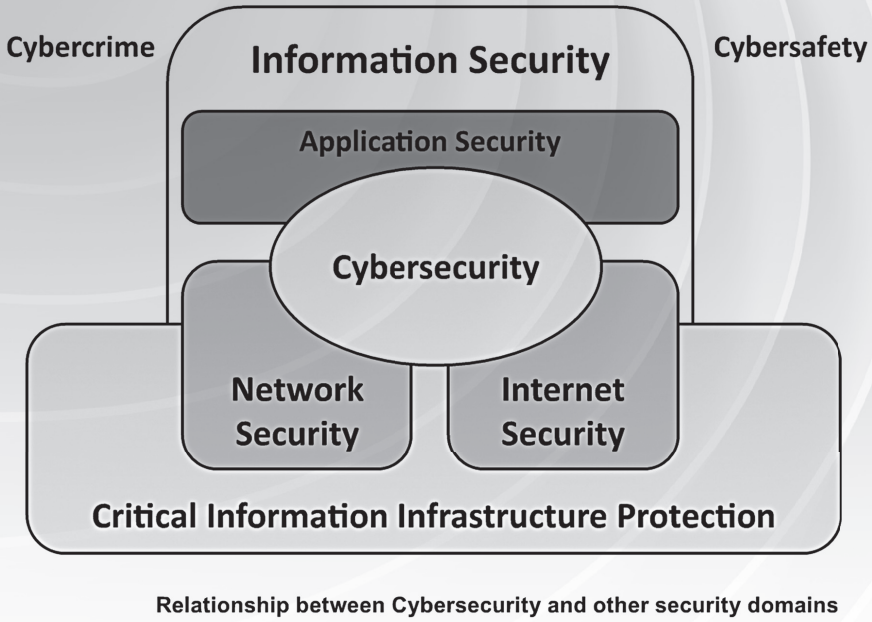
(๓) สื่อสารข้อกำหนดความต้องการด้านความมั่นคงปลอดภัยไซเบอร์กับผู้มีส่วนได้ส่วนเสีย

(๔) ระบุโอกาสในการจัดทำหรือทบทวนมาตรฐานและแนวปฏิบัติที่อ้างอิง

(๕) พิจารณาวิธีการเพื่อคุ้มครองสิทธิเสรีภาพและความเป็นส่วนตัว

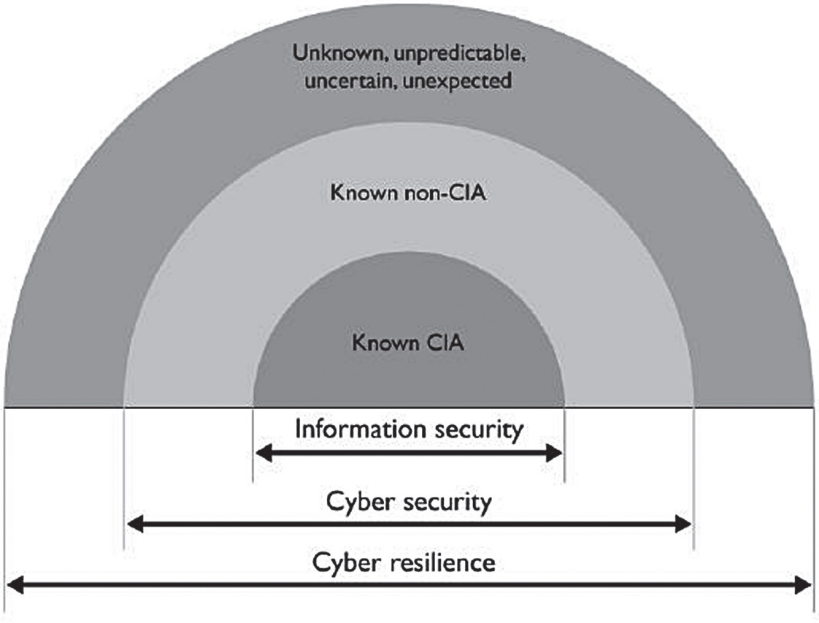
นอกจากนี้ โครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ (Framework Core) ตามกรอบการดำเนินงาน Cybersecurity Framework นี้ ยังสามารถแบ่งรายละเอียดลงไปในแต่ละหัวข้อของทั้ง ๕ Function เพื่อเชื่อมโยงข้อมูลอ้างอิง (Informative references) ซึ่งได้แก่ มาตรฐาน แนวปฏิบัติ หรือข้อกำหนดอื่นๆ ที่สามารถนำมาประยุกต์ใช้ในแต่ละ Function โดยไม่เพียงครอบคลุมการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบเทคโนโลยีสารสนเทศ แต่ยังมุ่งเน้นที่ระบบควบคุมอุตสาหกรรม (Industrial Control System: ICS) ซึ่งมีผลกระทบในวงกว้างมากกว่า ทำให้ผู้ใช้ในกลุ่มหน่วยงานระบบโครงสร้างพื้นฐานสำคัญจะได้รับประโยชน์อย่างเต็มที่ในการใช้กรอบการดำเนินงาน Cybersecurity Framework นี้ ซึ่งได้ประยุกต์และอ้างอิงกับมาตรฐานที่องค์กรส่วนใหญ่ได้ดำเนินการอยู่แล้ว อาทิ CCS CSC (Council on Cybersecurity: 20 Critical Security Controls), COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013 และ NIST SP 800-53 Rev.4 รวมทั้งกรอบการดำเนินงานด้านไซเบอร์โดย NIST (ดูเพิ่มเติม http://www.nist.gov/cyberframework/)

ในปัจจุบันและอนาคต หน่วยงานของรัฐและองค์กรต่าง ๆ จำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง ซึ่งการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) หรือด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security) นั้นไม่เพียงพอ ไม่ว่าจะเป็น Application Security, Network Security, Internet Security, Information Security หากแต่ต้องเป็น “Cybersecurity” ในภาพรวม พร้อมทั้งการป้องกันโครงสร้างพื้นฐานสำคัญตามแนวทาง CIIP (Critical Information Infrastructure Protection) (รูปที่ ๑๐ ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยที่เกี่ยวข้องไอที จาก มาตรฐาน ISO/IEC 27032:2012: Guideline for cybersecurity) โดยรวมถึงการจัดการเพื่อรองรับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Resilience) ในการรับมือกับภัยคุกคามความมั่นคงปลอดภัยที่ไม่อาจคาดคิด ที่ไม่แน่นอน ที่ไม่สามารถคาดการณ์ได้ และที่ไม่รู้ (unknown, unpredictable, uncertain, unexpected) (รูปที่ ๑๑ ความสัมพันธ์ระหว่าง Cyber Resilience, Cybersecurity and Information Security)



รูปที่ ๑๐ ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบสารสนเทศ

Source: "Relationship between Cybersecurity and other security domains" from ISO/IEC 27032:2012 : Guideline for cybersecurity



รูปที่ ๑๑ ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยด้านต่าง ๆ กับการรับมือภัยไซเบอร์

Source: "Relationship between Cyber Resilience, Cybersecurity and Information Security, ISF Threat Horizon Presentation

กล่าวโดยสรุปได้ว่า ถึงเวลาแล้วที่หน่วยงานของรัฐและองค์กรทุกองค์กร โดยเฉพาะอย่างยิ่งองค์กรในกลุ่มโครงสร้างพื้นฐานสำคัญ ซึ่งความมั่นคงปลอดภัยของระบบควบคุมอุตสาหกรรม (ICS) สำหรับระบบโครงสร้างพื้นฐานสำคัญขององค์กร มีผลกระทบทางกายภาพโดยตรงต่อสังคมและโลก รวมทั้งความเสี่ยงที่อาจเกิดขึ้นต่อสุขภาพและความปลอดภัยของประชาชน และผลกระทบต่อสิ่งแวดล้อม ผู้บริหารหน่วยงานของรัฐและองค์กรทุกองค์กรจำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ ซึ่งต้องมาจากวิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงขององค์กร (Top Management's Vision and Leadership) ที่ต้องให้เตรียมพร้อมรับมือ ดังคำที่ว่า "ป้องกันไว้ก่อน ดีกว่ามาแก้กันทีหลัง" ด้วยการมองหาแนวทางและโอกาสในการปรับปรุง (Opportunities for improvement: OFI) โดยการดำเนินการป้องกันไว้ก่อนในรูปแบบลักษณะเกราะกันภัย จากกรอบการดำเนินงานที่นำมาปฏิบัติใช้งานได้อย่างจริงจังและต่อเนื่อง ไม่ใช่มีเกราะกันภัยแต่ปล่อยไว้ไม่ใช้งานหรือใช้บ้างไม่ใช้บ้าง หรืออาจต้องมาตามแก้ไขจากภัยคุกคามและความเสี่ยงที่เกิดขึ้น ทั้งที่รู้และไม่รู้ (Known and Unknown Threat/Risk) โดยควรคำนึงถึง Zero Day Attack อยู่เสมอ เพราะการป้องกันที่ดี ย่อมทำให้พร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสมทันท่วงที แต่หากไม่มีการป้องกันที่ดี รอเหตุการณ์เกิดขึ้นก็อาจจะยากที่รับมือหรือแก้ไขได้ เมื่อถึงตอนนั้น ภัยคุกคามก็อาจจะเป็นความเสี่ยงที่ยากต่อการบริหารจัดการ เป็นความเสี่ยงที่กระทบต่อความอยู่รอดขององค์กรในระยะยาวและยากที่จะดำเนินธุรกิจแบบยั่งยืนได้ในที่สุด

อ้างอิง

[1] "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.0, National Institute of Standards and Technology, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, February 12, 2014.

[2] "The Critical Security Controls for Effective Cyber Defense" Version 5.0, Council on Cybersecurity, http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf, February 27, 2014.

[3] "อันดับแนวโน้มภัยคุกคามไซเบอร์ทั่วโลกประจำปี ๒๐๑๔ จากงานวิจัยสถิติของการประชุมเศรษฐกิจโลก" Global Agenda 2014, World Economic Forum, http://www.weforum.org/reports/outlook-global-agenda-2014.

[4] "แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยที่องค์กรทั่วโลกตระหนัก ปี ๒๐๑๔ งานวิจัยโดยสถาบัน BCI" Global Agenda 2014, Threats and Horizon Scanning 2014, The BCI, http://www.thebci.org/index.php/threats-and-horizon-scanning

[5] "ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบสารสนเทศ" Relationship between Cybersecurity and other security domains" from ISO/IEC 27032:2012 : Guideline for cybersecurity, http://www.iso.org/iso/catalogue_detail?csnumber=44375

[6] "ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยด้านต่าง ๆ กับการรับมือภัยไซเบอร์" Relationship between Cyber Resilience, Cybersecurity and Information Security, ISF Threat Horizon 2014, http://www.crypto-gen.com/pdf/2014-executive-summary.pdf