

5.) สแปม (Spam).....	50
6.) สแกนนิ่ง (Scanning).....	51
7.) บอตเน็ต (Botnet).....	54
8.) โอเพ่น ดีเอ็นเอส รีโซลเวอร์ (Open DNS Resolver).....	56
9.) โอเพ่น พร็อกซี เซิร์ฟเวอร์ (Open Proxy Server).....	57
4.3.2 สถิติ Incident ที่ได้รับแจ้งโดยตรง	58
4.4 สถานการณ์ด้านความมั่นคงปลอดภัย (Incident) ซึ่งเป็นกรณีศึกษาที่ไทยCERT เข้าไปดำเนินการ	67
4.4.1 การบุกรุกเข้าระบบจัดการโดเมนเนมของ T.H. NIC	68
4.4.2 การระบาดของมัลแวร์ดีเอ็นเอส เซนเจอร์ (DNS Changer Malware).....	69
4.4.3 การพบเครื่อง C&C ของ Malware ตระกูลเฟลม (Flame).....	70
4.4.4 การขโมยบัญชีผู้ใช้งานอีเมลของผู้ประกอบการประเภทยานยนต์.....	71
4.4.5 การแก้ไขปัญหา Phishing ในผู้ให้บริการเว็บโฮสติ้ง (Web Hosting) ของไทย...	72
5. CERTs กับ AEC 2015.....	75
5.1 CERTs พันธกรณีที่กำหนดไว้ในกรอบ AEC 2015	75
5.2 รายงาน CERTs ของประเทศสมาชิกอาเซียน.....	77
5.3 ความเข้มแข็งในการทำงานร่วมกันของ CERTs	81
5.3.1 การสร้างเครือข่ายความร่วมมือ	81
5.3.2 การกำหนดผู้ประสานงานหลัก (Point of Contact)	82
5.3.3 การให้ข้อมูลเกี่ยวกับภัยคุกคามด้านสารสนเทศ	82
5.3.4 การจัดทำมาตรฐานเกี่ยวกับข้อมูลภัยคุกคามด้านสารสนเทศ	82
5.3.5 การชักชวนรับมือภัยคุกคามด้านสารสนเทศ	83
5.3.6 การจัดเตรียมระบบเฝ้าระวังภัยคุกคามในเครือข่ายคอมพิวเตอร์ (Sensor Network).....	84
6. Threats กับ สิทธิในความเป็นส่วนตัว (Privacy).....	87
7. ประเทศไทยพร้อมหรือยังกับภัยคุกคามที่เกิดขึ้น	93
8. ภาคผนวก	97
8.1 ภาคผนวก ก การจัดประเภทของเหตุภัยคุกคามด้านสารสนเทศ	97
8.2 ภาคผนวก ข ตารางที่ 29 อภิธานศัพท์และคำย่อ.....	100
8.3 ภาคผนวก ค กฎหมายอนุบัญญัติที่มีมาตรการเกี่ยวกับความมั่นคงปลอดภัย.....	104
8.4 ภาคผนวก ง รายชื่อผู้ทรงคุณวุฒิและผู้ที่เกี่ยวข้องกับการผลักดัน เกี่ยวกับความมั่นคงปลอดภัย	108

สารบัญ

สารบัญ	8
สารบัญตาราง	10
สารบัญรูปภาพ	11
สารบัญกราฟ	12
บทนำ.....	15
1. “Cybersecurity” ภูมิบทของความเชื่อมั่นในการใช้ไอซีที	17
2. “IT Threats & Risks” กับสถานะและความพร้อมของประเทศไทย	21
3. ความเป็นมาของเครือข่าย CERTs และทีม ThaiCERT	29
4. รายงาน “Threats & Cybersecurity ปี 2555” ภายใต้บทบาท ThaiCERT	33
4.1 บริการของ ThaiCERT	33
4.1.1 บริการรับมือและจัดการสถานการณ์ ด้านความมั่นคงปลอดภัย	33
4.1.2 บริการข้อมูลข่าวสารความมั่นคงปลอดภัย	34
4.1.3 บริการวิชาการในการรักษาความมั่นคงปลอดภัย	34
4.2 การประสานเพื่อรับมือและจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย.....	35
4.2.1 การคัดแยกเรื่องที่ได้รับแจ้ง (Triage).....	35
4.2.2 การวิเคราะห์และจัดการภัยคุกคาม (Analyze and Handle)	36
4.2.3 การให้คำแนะนำในการแก้ปัญหา (Expert Opinion).....	36
4.2.4 การแจ้งเตือนและติดตามผล (Notification and Follow-up)	37
4.2.5 สรุปและแจ้งผลการจัดการ (Record and Feedback)	37
4.3 Threats ที่ไทยCERTรับแจ้งและดำเนินการ	37
4.3.1 สถิติ Incident ที่เกิดภายในประเทศไทยและได้รับแจ้งผ่านระบบอัตโนมัติ (Automatic Feed).....	39
1.) Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติปี 2555	
จำแนกตามประเภทภัยคุกคาม	40
2.) Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติแยกตามผู้ให้บริการ	
เครือข่ายในประเทศไทย	42
3.) ฟิชชิง (Phishing)	44
4.) มัลแวร์ ยูอาร์แอล (Malware URL).....	47