ความมั่นคงทางคอมพิวเตอร์ในการกำกับดูแลความปลอดภัยทางนิวเคลียร์และรังสี (Computer Security in Nuclear and Radiation Safety Regulation)

เรียบเรียงโดย นายชลกานต์ เอี่ยมสำอางค์
สำนักงานปรมาณูเพื่อสันติ

บทนำ

ในปัจจุบันความตระหนักในเรื่องของความมั่นคงทางคอมพิวเตอร์ยังมีอยู่ไม่มากเพียงพอภายในหน่วยงานที่ใช้ประโยชน์ทางนิวเคลียร์และรังสี ทั้งการใช้โปรแกรมที่ไม่ได้มาตรฐานหรือไม่มีลิขสิทธิ์ ไม่มีการจัดการการเข้าถึงข้อมูลที่รัดกุม และไม่มีกฎระเบียบบังคับโดยหน่วยงานกำกับดูแล ทำให้หน่วยงานมีความเสี่ยงสูงในการถูกโจมตีได้โดยบุคคลภายนอก ซึ่งข้อมูลที่สำคัญอาจถูกโจรกรรมหรือนำไปใช้ในทางที่ผิดได้โดยง่าย

ความมั่นคงทางคอมพิวเตอร์จึงเป็นสิ่งจำเป็นจะต้องมีมาตรการส่งเสริมและสร้างความตระหนัก มีการวิเคราะห์พัฒนาระเบียบด้านความมั่นคงทางคอมพิวเตอร์ของหน่วยงาน เพื่อให้มีการดำเนินการปรับปรุงและบังคับใช้ให้มีมาตรการป้องกันการโจมตีที่มีประสิทธิภาพ นอกจากนี้จึงควรมีการศึกษาพัฒนากฎระเบียบประกอบการขออนุญาตในด้านความมั่นคงทางคอมพิวเตอร์สำหรับหน่วยงานที่ใช้ประโยชน์จากพลังงานนิวเคลียร์และรังสี โดยมีการพัฒนาแนวทางการปฏิบัติที่เป็นมาตรฐาน และให้มีการประเมินมาตรการด้านความมั่นคงทางคอมพิวเตอร์เป็นส่วนหนึ่งของการประเมินความมั่นคงทางนิวเคลียร์ของสถานประกอบการ

หัวข้อหลักทางด้านความมั่นคงทางคอมพิวเตอร์ มีดังต่อไปนี้

1. ความตระหนักของภัยคุกคามและผลกระทบ (Threat and Consequence Awareness)
2. ความมั่นคงทางคอมพิวเตอร์ที่เกี่ยวข้องในงานด้านนิวเคลียร์และรังสี (Computer Security in Nuclear and Radiation Applications)
    - 2.1. ความมั่นคงทางคอมพิวเตอร์สำหรับระบบควบคุมทางอุตสาหกรรม (Computer Security for Nuclear IC Systems)
    - 2.2. ความมั่นคงทางคอมพิวเตอร์ในระบบรักษาความปลอดภัยและระบบเฝ้าระวังชายแดน (Computer Security Considerations for PPS and Border Monitoring Systems)
    - 2.3. ความมั่นคงทางคอมพิวเตอร์ของการเชื่อมโยงระหว่างอุปกรณ์ (Computer Asset-Node Security)
3. กฎหมายและนโยบายด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Law and Policy)
    - 3.1. โครงสร้างกฎหมายและกฎระเบียบด้านความมั่นคงทางคอมพิวเตอร์ (Legislative and Regulatory Frameworks for Computer Security)
    - 3.2. นโยบายด้านความมั่นคงทางนิวเคลียร์และการพัฒนาแผนการบริหารจัดการ (Computer Security Policy and Programme Development)
    - 3.3. การวิเคราะห์และบริหารความเสี่ยง (Risk Assessment and Management)
    - 3.4. การออกแบบและบริหารความมั่นคงทางคอมพิวเตอร์ (Computer Security Design and Management)

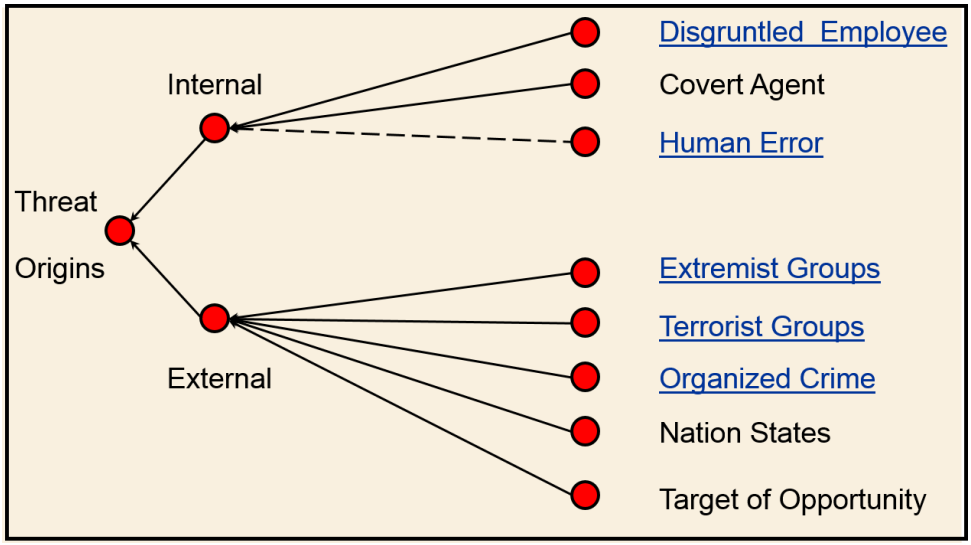
4. การบริหารจัดการด้านความมั่นคงทางคอมพิวเตอร์ภายในองค์กร (Computer Security Management)
   4.1. ภัยคุกคามจากบุคคลภายใน (The Insider Threat)
   4.2. วัฒนธรรมด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Culture)
   4.3. การบริหารจัดการบุคลากรด้านความมั่นคง (Human Resource Management and Personnel Security)
5. การตอบสนองต่อเหตุการณ์ด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Incident Response)

1. ความตระหนักของภัยคุกคามและผลกระทบ (Threat and Consequence Awareness)

สิ่งที่สำคัญต่อการรับมือการโจมตีทางไซเบอร์ คือการทำความเข้าใจถึงประเภทของการคุกคามทางไซเบอร์ และศึกษาเหตุการณ์ที่เคยเกิดขึ้น เพื่อทราบถึงแนวโน้มของเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต

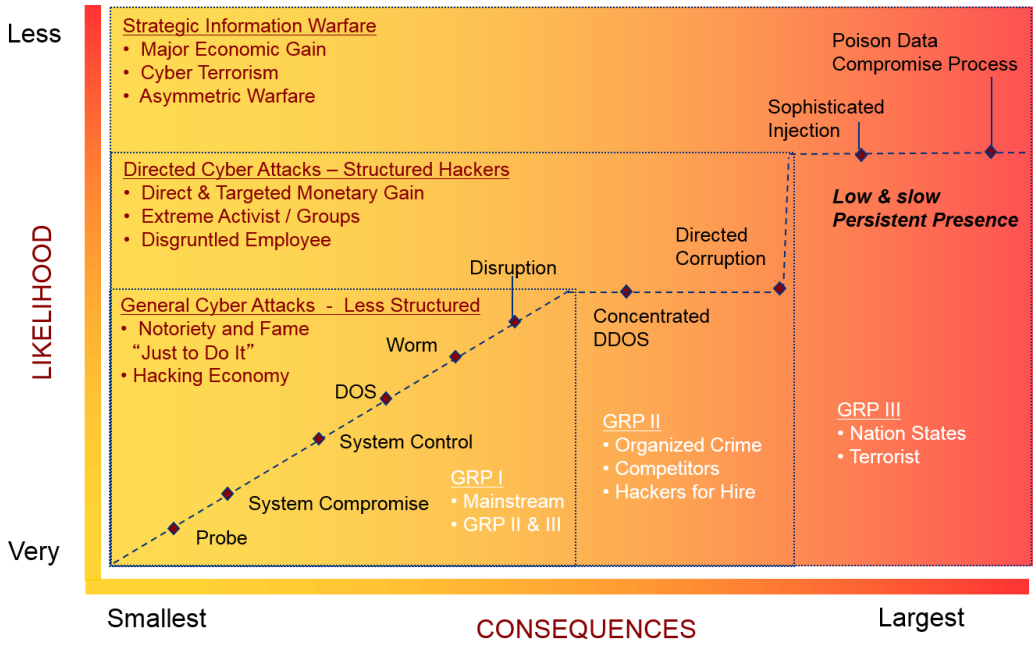
ประเภทของผู้กระทำการภัยคุกคามทางไซเบอร์แบ่งออกเป็น

- ภายใน (Internal)
  - Disgruntled Employee
  - Covert Agent
  - Human Error
- ภายนอก (External)
  - Extremist Groups
  - Terrorist Groups
  - Organized Crime
  - Nation States
  - Target of Opportunity



Threat = capability + intent + opportunity

ภัยคุกคาม (threat) เกิดจากการประกอบกันของ สมรรถนะ (capability) เจตนา (intent) และโอกาส (opportunity)



ลักษณะทั่วไปของภัยคุกคามทางไซเบอร์แบ่งออกได้เป็น 2 ลักษณะ ดังนี้

1. ความน่าจะเป็นจะเกิดขึ้น (likelihood)
    - General Cyber Attacks – Less Structured
    - Directed Cyber Attacks – Structured Hackers
    - Strategic Information Warfare
2. ผลกระทบ (consequences)
    - Group I – Mainstream
    - Group II – Organized Crime, Competitors, Hackers for Hire
    - Group III – Nation States, Terrorist

โดยภัยคุกคามที่มีความน่าจะเป็นมากและผลกระทบน้อย คือพวก Worm, DDOS, Disruption และภัยคุกคามที่มีความน้อยและผลกระทบมาก คือพวก Poison Data, Compromise Process, Sophisticated Injection

ทางด้านนิวเคลียร์ เป้าหมายของภัยคุกคามทางไซเบอร์คือสถานประกอบการทางนิวเคลียร์ เช่น

- Monju NPP (Japan) – Compromise of control room computer and release of information (2014)
- Korea Hydro and Nuclear Power (KHNP) – Computer compromise and release of NPP documents (2014)
- Gundremmingen NPP (Germany) – Computer virus's found on plan IT systems and media (2016)

ซึ่งแนวโน้มของภัยคุกคามจะมีมากขึ้นเรื่อยๆ เนื่องจากมีจำนวนอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตมากขึ้นเรื่อยๆ ทำให้จำนวนผู้ก่อการร้ายมีมากขึ้น มีการรับจ้าง การทำการที่ซับซ้อนมากขึ้น และมีความรุนแรงมากขึ้น ซึ่งภัยคุกคามที่จะมีมากคือพวก spear phishing และ ransomeware

ตัวอย่างภัยคุกคามที่เกิดขึ้นไม่นานมานี้ คือ

1. Red October (January 2013)
2. Heartbleed (April 2014)

เป้าหมายของภัยคุกคามที่อาจเกิดขึ้นทางด้านนิวเคลียร์ คือ transportation, supply chain, industrial control systems

โดยกระบวนการการคุมคามทางไซเบอร์แบ่งออกเป็น 5 ขั้นตอน

Phase 1: Reconnaissance (เก็บข้อมูล)
Phase 2: Target Identification (กำหนดเป้าหมาย)
Phase 3: Computer System Compromise (เข้าถึงจุดอ่อนในระบบ)
Phase 4: Attack Execution (ทำการโจมตี)
Phase 5: Asserting Deniability (ทำลายหลักฐาน)

2. ความมั่นคงทางคอมพิวเตอร์ที่เกี่ยวข้องในงานด้านนิวเคลียร์และรังสี (Computer Security in Nuclear and Radiation Applications)

2.1. ความมั่นคงทางคอมพิวเตอร์สำหรับระบบควบคุมทางอุตสาหกรรม (Computer Security for Nuclear IC Systems)

Industrial Control System (ICS) คือชื่อที่ใช้เรียกระบบควบคุมต่าง ๆ ทั้ง analog และ digital ที่ใช้ในการผลิตทางอุตสาหกรรม รวมถึง Supervisory Control and Data Acquisition (SCADA) และ Distributed Control System (DCS) ซึ่งปกติแล้วจะประกอบไปด้วยอุปกรณ์ Instrumentation and Control (I&C) เช่น sensors and transmitters, controllers, control elements, human machine interface

ในทางนิวเคลียร์ ICS หรือ I&C จะเป็นส่วนสำคัญที่สนับสนุนการทำงานของอุปกรณ์ของระบบที่เกี่ยวกับการควบคุมความปลอดภัย ตัวอย่างของระบบที่ต้องใช้ ICS เป็นส่วนประกอบมีดังนี้

Primary Systems

- Reactivity Control Systems
- Reactor Coolant System
- Steam Generator System
- Pressurizer System
- Emergency Core Cooling Systems
- Reactor Protection System
- Engineered Safeguard Feature Actuation System

Secondary Systems

- Turbine System
- Main Generator System
- Condenser System

- Feedwater System
- Auxiliary / Emergency Feedwater System
- Fire Protection System
- Emergency Power Supply Systems

Security Systems

- Access Control
- Video Surveillance
- Intrusion Detection
- Metal Detection
- Explosive Detection
- X-Ray Systems

Emergency Response

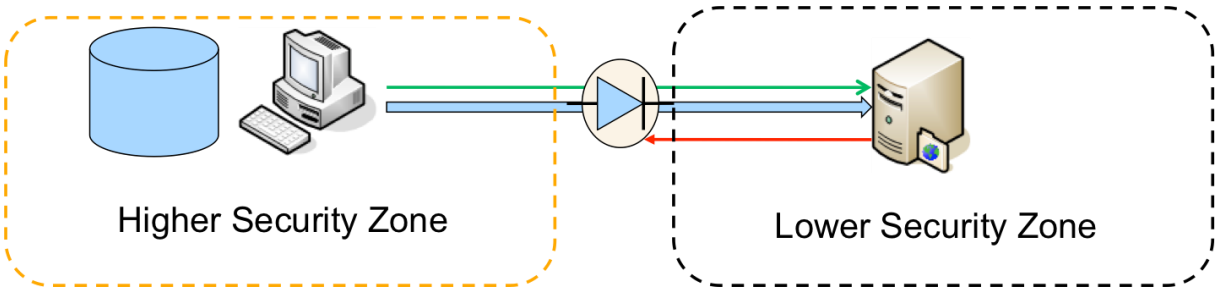
- Meteorological Systems
- Siren Systems
- Radiation Monitoring Systems

จุดอ่อนทั่วไปของ ICS ที่สามารถถูกโจมตีได้มาจาก การไม่เปลี่ยนรหัสผ่าน การใช้รหัสผ่านร่วมกัน การไม่มีระบบควบคุมความมั่นคง การบริหารจัดการโปรแกรมที่ไม่ดี การเข้าระบบอัตโนมัติ การไม่ตรวจสอบบันทึกการใช้งาน การเข้าใช้ระบบจากนอกสถานที่ เป็นต้น

ปัญหาหลักของ ICS ในปัจจุบันคือ ระบบไม่มีการตรวจสอบความน่าเชื่อถือ (authentication) ไม่มีกำลังเพียงพอที่จะลงโปรแกรมป้องกันไวรัส ไม่มีการเข้ารหัส (encryption) ไม่มีการบันทึกการใช้งาน (logging) ไม่มีการป้องกันทางกายภาพ ไม่มีการ update patch และไม่มีระบบเครือข่ายที่มั่นคง

วิธีการป้องกันการถูกโจมตี เริ่มต้นจากการตรวจสอบและแบ่งประเภทการทำงานของ ICS ตามความสำคัญที่จะมีผลกระทบต่อความปลอดภัยของระบบ แล้วจึงจัดการการป้องกันตามระดับนั้นๆ โดยวิธีการมีดังต่อไปนี้

1. ต้องมี firewall ในระบบ
2. ระบบที่สำคัญต้องเป็น one-way communication (data diode)
3. มีการทำ white list ของโปรแกรมที่อนุญาตให้ใช้ได้
4. มีการจัดทำการวิเคราะห์ประเมินความเสี่ยงของการถูกโจมตี



2.2. ความมั่นคงทางนิวเคลียร์ในระบบรักษาความปลอดภัยและระบบเฝ้าระวังชายแดน (Computer Security Considerations for PPS and Border Monitoring Systems)

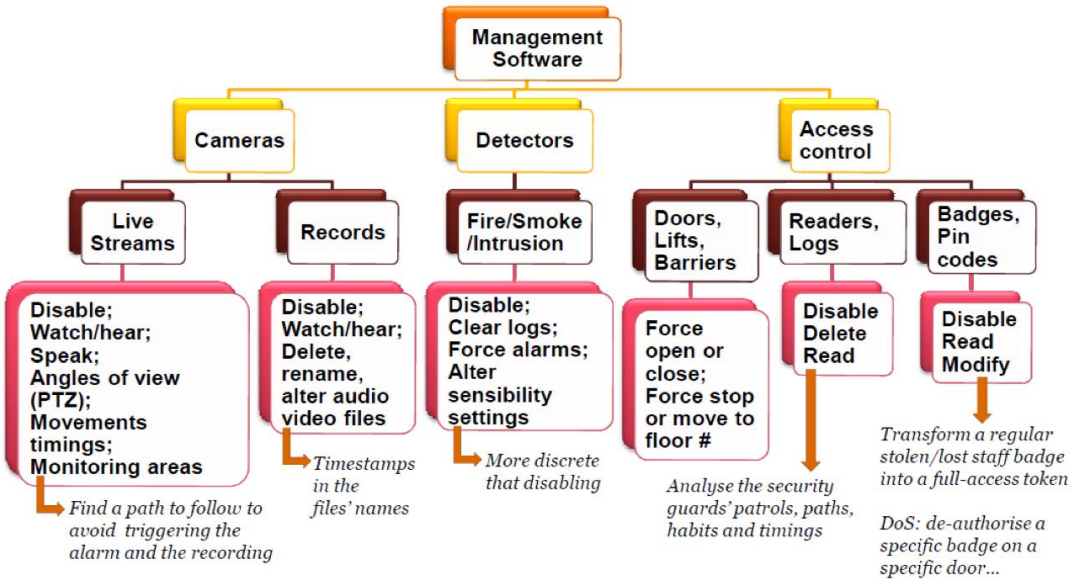
Physical Protection System (PPS) เป็นระบบที่ใช้เพื่อป้องกันภัยอันตรายจากการขโมย การทำลาย และการทำอันตรายต่อสถานประกอบการทางหรือยานพาหนะ PPS ประกอบไปด้วยอุปกรณ์ทางเทคนิคที่ใช้ในการค้นหา (detection) เตือนภัย (alarm) และสอดส่องดูแล (surveillance) ซึ่งในปัจจุบันอุปกรณ์เหล่านี้ถูกเชื่อมโยงด้วยเครือข่ายกับเครื่องคอมพิวเตอร์ทั่วไปที่อาจจะถูกโจมตีได้

ส่วนประกอบหลักของ PPS แบ่งออกเป็น ดังนี้

1. Sensor suite ซึ่งมีหลากหลายแบบเพื่อใช้ในการตรวจจับการการสั่นสะเทือน การเปิดปิดประตูหน้าต่าง ความร้อนจากร่างกายด้วยคลื่นอินฟราเรด การเคลื่อนไหวจากคลื่นอัลตราโซนิคหรือไมโครเวฟ แรงกดบนพื้น และการจับภาพเคลื่อนไหว
2. Alarm processor ประกอบไปด้วย signal routing เพื่อส่งสัญญาณเพื่อนำไปประมวลผล และ alarm processing เพื่อวิเคราะห์สัญญาณที่ได้รับ
3. Alarm display ทำหน้าที่รับผลที่ผ่านการประมวลแล้วมาแสดงบนเครื่องคอมพิวเตอร์

โดยทุกส่วนประกอบต้องได้รับการป้องกันทั้งทางกายภาพและทางการควบคุมผ่านเครือข่าย รวมทั้งอุปกรณ์ USB และ CD/DVD เพื่อไม่ให้โปรแกรมโจมตีสามารถเข้าถึงได้

เป้าหมายที่อาจถูกโจมตีได้ใน PPS มีดังนี้



ในส่วนของการเฝ้าระวังชายแดนเพื่อป้องกันการเคลื่อนย้ายวัสดุกัมมันตรังสีเข้าออกโดยผิดกฎหมาย หน่วยงานที่รับผิดชอบจะต้องดำเนินการเตรียมพร้อมรับมือเพื่อตรวจจับ รวมถึงการรับมือทางด้านการคุกคามทางไซเบอร์ ซึ่งอุปกรณ์หลักที่ใช้จะแบ่งออกเป็น

- Fixed-installed:
  - Radiation Portal Monitor (RPM) เช่น Pedestrian RPM, Train RPM, Mobile RPM ซึ่งสามารถตรวจจับได้ถึง 70% ตามข้อมูล IAEA Illicit Trafficking Database
- Handhelds:

- Personal Radiation Detector (PRD) เครื่องมือตรวจจับขนาดเล็ก
- Radionuclide Identification Device (RID) เครื่องมือขนาดพกพาเพื่อใช้ตรวจวัดรังสี และเก็บค่า dose rate
- Neutron Search Detector (NSD) เครื่องมือวัดที่มีประสิทธิภาพสูงในการตรวจนับนิวตรอน

โดยอุปกรณ์เหล่านี้จะต้องอยู่ภายใต้ Integrated Nuclear Security Network (INSN) ซึ่งสามารถถูกโจมตีได้ เพราะเป็นการเชื่อมโยงผ่านเส้นทางสื่อสารที่เป็นของเอกชน และผ่านการทำงานร่วมกันของหลากหลายหน่วยงานที่ทำให้เกิดจุดอ่อน นอกจากนี้ การเก็บของมูลด้วยอุปกรณ์เคลื่อนที่ เปิดช่องให้มีการทำลายข้อมูลระหว่างการเคลื่อนย้ายและส่งข้อมูล

2.3. ความมั่นคงทางคอมพิวเตอร์ของการเชื่อมโยงระหว่างอุปกรณ์ (Computer Asset-Node Security)

สิ่งสำคัญในการบริหารจัดการอุปกรณ์คอมพิวเตอร์ (asset) ที่มีอยู่คือ ต้องเข้าใจข้อมูลทั้งหมดของระบบที่มีอยู่ เข้าใจการเชื่อมโยงระหว่างอุปกรณ์ และเข้าใจผลกระทบระหว่างระบบด้านความปลอดภัยและด้านความมั่นคง โดยการดำเนินการต้องแบ่งตามลำดับความสำคัญ (graded approach) และการบริหารจัดการต้องทราบถึงความเสี่ยงทั้งหมด

ศัพท์ที่ควรจะรู้คือ

- Critical Systems (CS) คือระบบที่ถ้าถูกโจมตีจะมีผลต่อความปลอดภัย ความมั่นคง และการตอบสนองต่อเหตุฉุกเฉินของสถานประกอบการทางนิวเคลียร์
- Non-Critical Systems (Non-CS) คือระบบถ้าถูกโจมตีจะไม่มีผลอย่าง CS
- Computer Essential Asset (CEA) คืออุปกรณ์คอมพิวเตอร์ที่เป็นส่วนประกอบสำคัญของ Critical Systems

การที่จะระบุว่าอะไรคือ CS และ CEA ทำได้โดย

1. ตรวจสอบว่าระบบใดเป็นระบบ CS
2. ตรวจสอบอุปกรณ์คอมพิวเตอร์และการทำงานของอุปกรณ์ที่เป็นส่วนหนึ่งของ CS
3. แบ่งกลุ่มอุปกรณ์คอมพิวเตอร์ให้เป็น CEA
4. ทำการวิเคราะห์ผลกระทบความเสียหายของแต่ล่ะ CEA ถ้าถูกโจมตี

วิธีปรับปรุงมาตรการความปลอดภัยทำได้โดยกระบวนการที่เรียกว่า Hardening

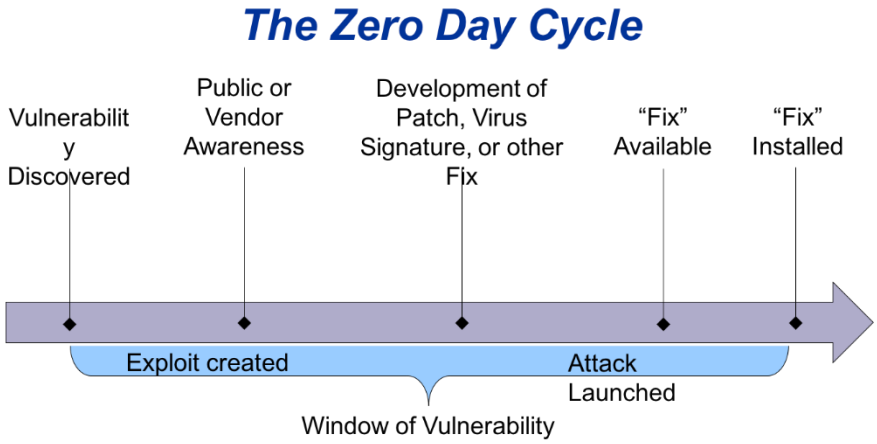
Hardware Hardening

- ปิดการติดต่อทาง wireless
- ปิดการติดต่อไปยังเครื่องข่ายที่ไม่ secure
- ปิดการใช้งาน USB
- ปิดการเขียนลง removable media (floppy/CD/DVD)
- จำกัดการอ่านข้อมูลจาก removable media

Software Hardening

- จัดทำมาตรการ access control
- ใช้ software จากบริษัทที่ไว้ใจได้
- มีการติดตั้งโปรแกรม antivirus
- มีการบันทึกการใช้งาน (event logging)
- จำกัดการโหลดโปรแกรมจากอินเทอร์เน็ต
- จัดการเอาโปรแกรมที่ไม่จำเป็นออกจากเครื่อง

นอกจากนี้จะต้องมีการบริหารจัดการ patch คือโปรแกรมจะต้องได้รับการ update อยู่ตลอดเวลา เพื่อมีการแก้ไข bug และปรับปรุงประสิทธิภาพการทำงาน ซึ่งถ้ามีการค้นพบจุดอ่อนของโปรแกรม แล้วไม่มีการปรับปรุงได้ทัน ก็จะทำให้ระบบถูกโจมตีได้ โดยช่วงเวลาที่ผู้โจมตีค้นพบจุดอ่อนจนถึงเวลาที่มีการปรับปรุงโปรแกรม ช่วงนี้จะเรียกว่าช่วง “zero day”



3. กฎหมายและนโยบายด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Law and Policy)

3.1. โครงสร้างกฎหมายและกฎระเบียบด้านความมั่นคงทางคอมพิวเตอร์ (Legislative and Regulatory Frameworks for Computer Security)

เอกสารของ IAEA ที่เกี่ยวของกับการทำกฎระเบียบด้าน Computer Security มีดังนี้

1. Nuclear Security Fundamentals (NSS20) กล่าวถึงหน้าที่ของรัฐในการวางกฎระเบียบและทำการป้องกันข้อมูลที่สำคัญ

2. Security of Nuclear Information (NSS 23-G) ให้คำแนะนำในการดำเนินการตามหลักการของ การรักษาความลับ (confidentiality) การคงสภาวะปกติ (integrity) และการมีความพร้อมอยู่เสมอ (availability)
3. Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) กล่าวถึงการป้องกันระบบที่ใช้คอมพิวเตอร์ สำหรับ physical protection, nuclear safety และ nuclear material accountancy and control ว่าต้องป้องกันต่อภัยคุกคามที่อาจเกิดขึ้น หรือ design basis threat
4. Computer Security at Nuclear Facilities (NSS 17) เพื่อสร้างความตระนักถึงความสำคัญของ computer security ต่อสถานประกอบการทางนิวเคลียร์ และแนะนำในการวางแผนป้องกัน และการบริหารอุปกรณ์ด้านข้อมูลและ I&C

กฎระเบียบด้านนิวเคลียร์จะต้องมีการเชื่อมโยงกับกฎระเบียบด้าน computer security ในส่วนของการทำผิด การก่อการร้าย การป้องกันโครงสร้างพื้นฐานที่สำคัญของประเทศ การป้องกันข้อมูลความลับ และการรักษาข้อมูลส่วนตัว โดยทางหน่วยงานที่รับผิดชอบจะต้องนิยามความหมายของคำว่า cyber attack, cyber crime และ cyber terrorism ให้ชัดเจน

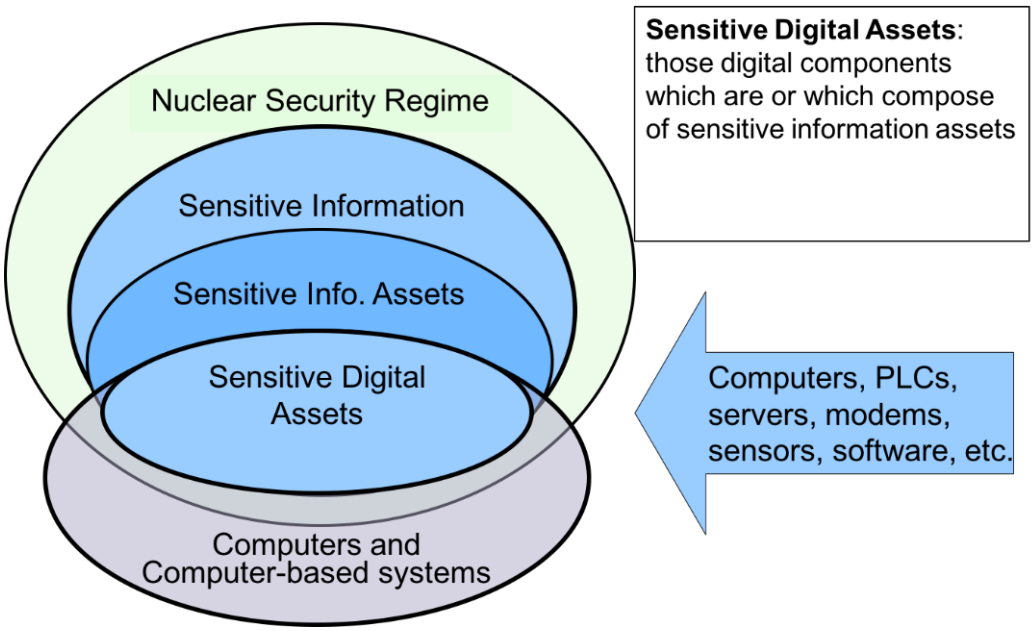
อนุสัญญาที่สำคัญทางด้านนี้คือ Budapest Convention on Cybercrime (November 2011) ซึ่งได้กำหนดสิ่งให้รัฐดำเนินการให้มีกฎหมายทางอาญาที่ครบถ้วนสมบูรณ์ (substantive criminal law) ต่อการกระทำ ดังต่อไปนี้

1. Illegal access การเข้าถึงข้อมูลที่ผิดกฎหมาย
2. Illegal interception การดักเก็บข้อมูลที่ผิดกฎหมาย
3. Data interference การแทรกแซงข้อมูล
4. System interference การแทรกแซงระบบ
5. Misuse of devices การใช้อุปกรณ์ไปในทางมิชอบ

3.2. นโยบายด้านความมั่นคงทางนิวเคลียร์และการพัฒนาแผนการบริหารจัดการ (Computer Security Policy and Programme Development)

จุดมุ่งหมายหลักของการจัดการความมั่นคงทางคอมพิวเตอร์มีดังต่อไปนี้

1. ป้องกันข้อมูลที่สำคัญ
2. ป้องกันสถานประกอบการทางนิวเคลียร์
3. ป้องกันวัสดุกัมมันตรังสีและวัสดุนิวเคลียร์
4. ป้องกันวัสดุกัมมันตรังสีและวัสดุนิวเคลียร์ที่อยู่นอกเหนือการควบคุม



ซึ่งจุดมุ่งหมายเหล่านี้อาจจะไม่เหมือนจุดมุ่งหมายเพื่อการบริหารจัดการ และอาจไม่เหมือนกับจุดมุ่งหมายเพื่อความปลอดภัย ดังนั้นจึงควรตรวจดูให้แน่ใจว่าจุดมุ่งหมายทางความมั่นคงจะไม่มีผลกระทบกับความปลอดภัย

สิ่งสำคัญในการจัดทำนโยบายด้านความมั่นคงทางคอมพิวเตอร์มีดังต่อไปนี้

1. ได้รับการสนับสนุนและบังคับใช้โดยผู้บริหารระดับสูง
2. ประกอบร่วมไปกับนโยบายด้านความมั่นคงทั้งหมดของหน่วยงาน
3. เผยแพร่และประกาศให้ทุกคนทราบโดยทั่วกัน
4. มีการทบทวนเนื้อหาอยู่เสมอ
5. ดำเนินการโดยให้มีคู่มือและขั้นตอนแนะนำ

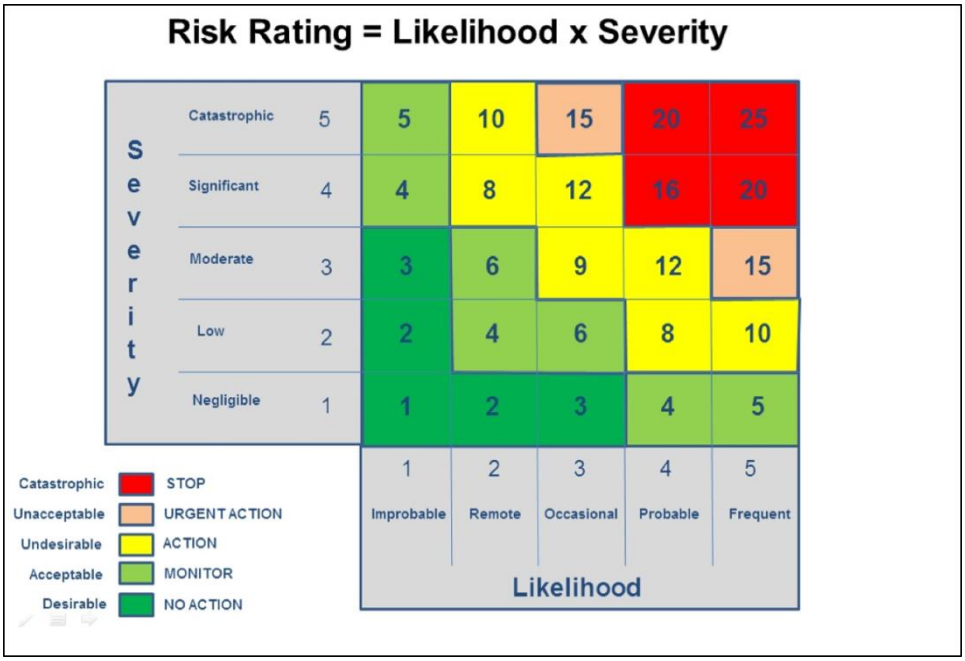
ควรมีการกำหนดตำแหน่งและหน้าที่ให้ชัดเจน เช่น มีการแต่งตั้งเจ้าหน้าที่ด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Officer; CSO) เป็นผู้ที่มีความรู้ทั้งทางด้านความมั่นคงทางคอมพิวเตอร์และความมั่นคงของสถานประกอบการทางนิวเคลียร์ รวมทั้งสามารถบริหารจัดการโครงการร่วมกันระหว่างบุคลากรจากหลายๆ หน่วยงาน

โดยผู้มีส่วนได้ส่วนเสีย (stakeholders) ทั้งหมดของสถานประกอบการทางนิวเคลียร์ ต้องมีการจัดทำแผนความมั่นคงทางคอมพิวเตอร์ (Computer Security Plan; CSP) เพื่อที่จะดูแลความปลอดภัยของข้อมูลสำคัญ ซึ่งส่วนประกอบ ของ CSP อย่างน้อยที่สุด ต้องประกอบไปด้วย

- Organization and responsibilities
- Asset management
- Risk, vulnerability, and compliance assessment
- System security design and configuration management:
- Operational security procedures
- Personnel management

3.3. การวิเคราะห์และบริหารความเสี่ยง (Risk Assessment and Management)

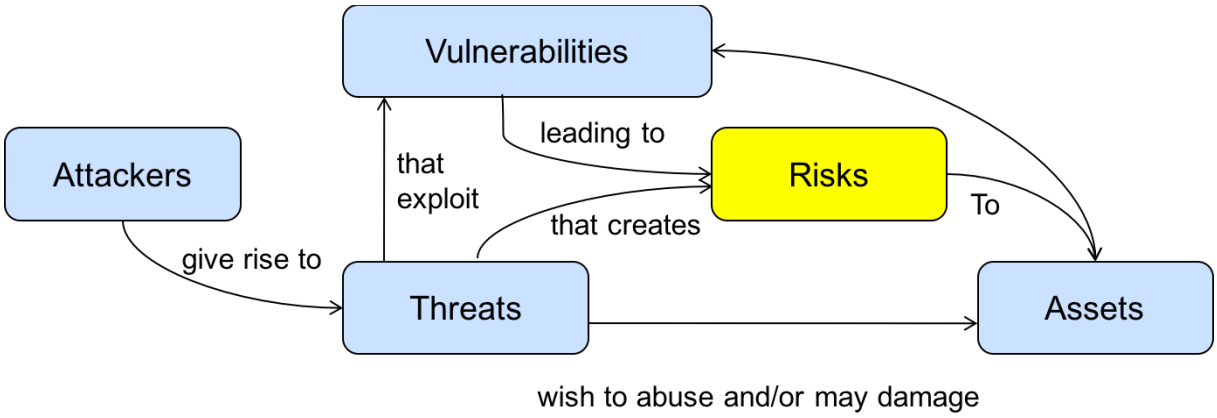
ความเสี่ยง (risk) คือความเป็นไปได้ที่ภัยคุกคามจะโจมตีจุดอ่อน ซึ่งเป็นฟังชั่นของ ความน่าจะเป็น (likelihood) และผลกระทบ (consequences) โดยการจัดลำดับความเสี่ยงจะสามารถทำให้เปรียบเทียบความสำคัญ โดยเครื่องมือหนึ่งคือการจัดทำ risk matrix



ในด้านความมั่นคงทางนิวเคลียร์ ความเสี่ยงที่เป็นจุดสนใจของเราคือ ความเสี่ยงที่เกิดจากภัยคุกคามจากเจตนามุ่งร้าย เช่น การโจรกรรม การทำลายล้าง การสร้างความเสียหาย โดย ต้นกำเนิดของภัยคุกคามที่แตกต่างกันก็จะมีจุดมุ่งหมายและความสามารถที่แตกต่างกัน

Threat Source	Intentions	Capabilities
Nation State	Intelligence collection Sabotage Technology theft	Strong resources Expertise Custom tools Insiders
Organized Crime	Theft Extortion Illicit trafficking	Strong resources Hired hackers Personal threats Insiders
Terrorist	Fear, Political instability Social disruption Overt damage to infrastructures	Varied resources Possible insiders Radical determination Violence of actions
Extremists	Influence public opinion Influence political policy	Varied skills
Disgruntled Employee	Revenge Theft/Disruption/Damage	Inside knowledge Existing access Professional training Internal authority
Recreational Hackers	Fun, status, challenge	Varied skills Limited resources

จุดอ่อน (vulnerability) คือส่วนต่างๆ ที่ไม่มั่นคงในระบบสารสนเทศ กระบวนการรักษาความปลอดภัย การควบคุมภายใน และการดำเนินการ ที่สามารถถูกโจมตีได้โดยผู้ประสงค์ร้าย



ดังนั้นจึงควรมีการจัดทำการวิเคราะห์ความเสี่ยง (risk analysis) โดยมีขั้นตอนดังต่อไปนี้

1. System/Asset Characterization เพื่อกำหนดขอบเขตของเป้าหมาย ข้อจำกัด เวลา และทรัพยากรที่มีอยู่
2. Threat Source Identification เพื่อระบุภัยคุกคามและผู้โจมตี รวมทั้งความรุนแรง
3. Threat Event Analysis เพื่อวิเคราะห์จุดอ่อนและความเชี่ยวชาญด้านความมั่นคงที่จำเป็น
4. Vulnerability Identification เพื่อประเมินจุดอ่อนด้วยตัวเองและจากภายนอก
5. Security Control Analysis เพื่อวิเคราะห์ว่าสามารถรับมือแผนการโจมตีที่ระบุได้หรือไม่ ในด้านการป้องกัน การตรวจจับ และการบรรเทาการโจมตีนั้นๆ
6. Likelihood Estimation เพื่อคำนวณความน่าจะเป็นที่การโจมตีจะสำเร็จ และความน่าจะเป็นที่การโจมตีจะทำให้เกิดความเสียหาย
7. Impact Analysis เพื่อวิเคราะห์ความเสียหายที่จะเกิดขึ้น หากการโจมตีนั้นสำเร็จ

เมื่อนำมาคำนวณรวมกันก็จะได้ผลการวิเคราะห์ความเสี่ยง

Threat Event									
Deliver targeted Trojan for control of internal systems Adversary manages to install software containing Trojan horses that are specifically and exfiltration of data.									
2	3	4	5	6	7	8	9	10	11
Threat Source	**Threat Source Capabilities**			**Likelihood of Action**	**Vulnerability**	**Likelihood of attack success**	**Overall likelihood**	**Level of Impact**	**Risk Score**
	Capability	**Intent**	**Targeting**						
Reference Table	D3	D4	D5	G2	F2	G4	G5	H3	I3
Extremist Group	L	L	L	VL	M	VL	VL	M	VL
Terrorist Group	L	VH	H	L	M	VL	VL	M	VL
Nation State	H	M	VH	M	M	M	L	M	M

หลังจากที่ได้ผลวิเคราะห์ความเสี่ยงมาแล้ว จากนั้นจะเป็นขั้นตอนในการใช้ผลที่ได้มาเพื่อในการช่วยในการตัดสินใจ (risk decision support) ในการบริหารความเสี่ยง (risk management) โดยมีขั้นตอนดังต่อไปนี้

1. Requirements definition/review เพื่อกำหนดระดับของความมั่นคงที่หน่วยงานจำเป็นต้องมีเพื่อป้องกันภัยคุกคาม
2. Security control identification เพื่อกำหนดแนวทางควบคุมความมั่นคง
3. Review of controls เพื่อทบทวนดูว่าแนวทางควบคุมนั้นเพียงพอหรือไม่
4. Mitigation strategy selection เพื่อเลือกแผนการบรรเทาเหตุที่อาจเกิดขึ้น

โดยแนวทางการจัดการกับความเสี่ยงที่มี สามารถทำได้โดยการ เปลี่ยนแปลงความเสี่ยง (risk modification) การควบคุมความเสี่ยง (risk retention) การลีกเลี่ยงความเสี่ยง (risk avoidance) และกระจายความเสี่ยง (risk sharing)

3.4. การออกแบบและบริหารความมั่นคงทางคอมพิวเตอร์ (Computer Security Design and Management)

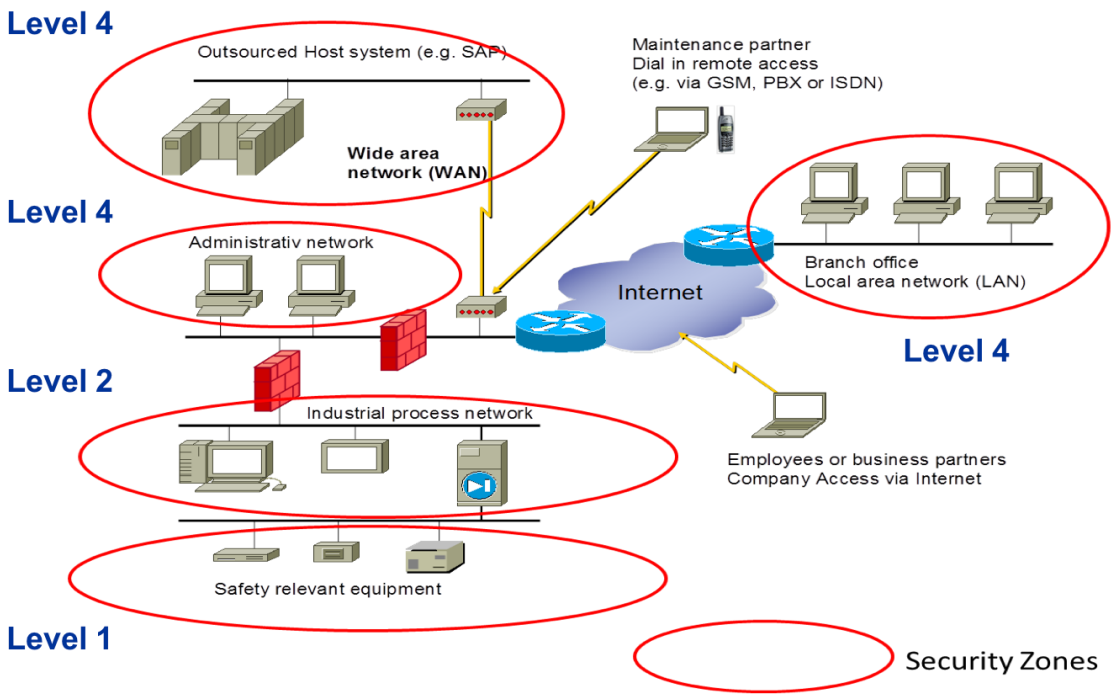
คำถามที่ควรจะถามในเรื่องของการรักษาความมั่นคงคือ “ภัยคุกคามระดับไหนที่ระบบรักษาความมั่นคงที่มีอยู่สามารถป้องกันได้” ทำให้ต้องมีการศึกษาวิเคราะห์ Design Basis Threat (DBT) เพื่อที่จะศึกษาภัยคุกคามที่อาจเกิดขึ้นและใครจะเป็นผู้กระทำ โดยมีเนื้อหาดังต่อไปนี้

1. Potential Adversaries ใครคือผู้ที่อาจโจมตี
2. Unacceptable Consequences ผลกระทบความเสียหายที่อาจเกิดขึ้น
3. Adversary Capabilities ความสามารถและเจตนาของผู้โจมตี
4. Protection Requirement มาตรการป้องกันที่จำเป็น

นอกเหนือจาก DBT การออกแบบมาตรการความมั่นคงต้องคิดถึงสิ่งเหล่านี้ รวมทั้งต้องคำนึงถึงความเหมาะสมและทฤษฎีการป้องกันหลายชั้น (defense in depth)

- Site functions/plans/sensitive asset inventory
- Site usability and worker ingress and egress
- Planning constraints and permissions
- Guard and security force requirements
- Safety policy and practice (and conflicting requirements)
- Emergency preparedness requirements
- Transport interfaces
- Working practices
- Personnel security
- Protecting key control rooms including the security control room
- Supply chain security considerations

การออกแบบสามารถใช้วิธีการแบ่งเป็นโซน (zone model protection) โดยแต่ละโซนต้องประกอบไปด้วยระบบที่มีความสำคัญใกล้เคียงกัน ต้องการเครื่องมือป้องกันที่คล้ายๆกัน และภายในโซนสามารถติดต่อกันได้ด้วยความเชื่อมั่น (trusted zone)



โดยให้มีการแบ่งระดับความปลอดภัยเป็นลำดับชั้น และให้มีมาตรการตามลำดับความสำคัญ

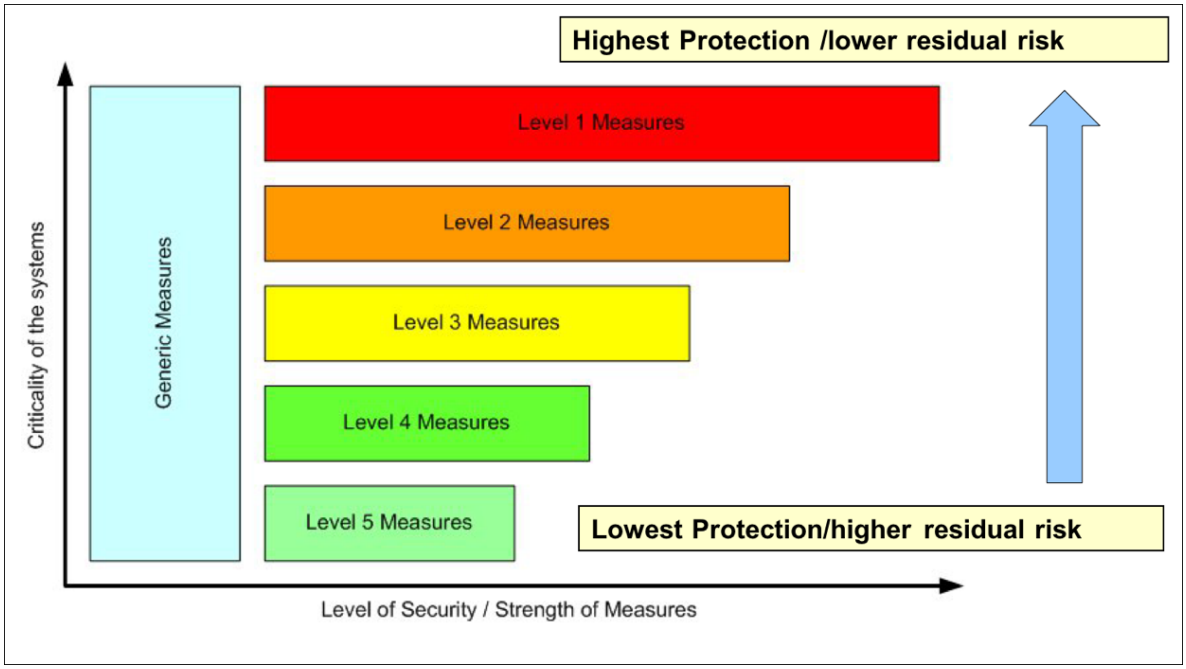
Level 5: ระบบที่ไม่มีความสำคัญโดยตรงต้องการบริหารจัดการและดำเนินการ

Level 4: ระบบที่มีข้อมูลทางเทคนิคสำหรับการซ่อมบำรุงและการดำเนินการ

Level 3: ระบบที่ดูแลการทำงานโดยตรงตลอดเวลาของระบบที่ไม่จำเป็นสำหรับการดำเนินการ

Level 2: ระบบที่ใช้ควบคุมดูแลการดำเนินการที่ต้องการการป้องกันระดับสูง

Level 1: ระบบที่ใช้ควบคุมดูแลการดำเนินการที่ต้องการการป้องกันระดับสูงที่สุด

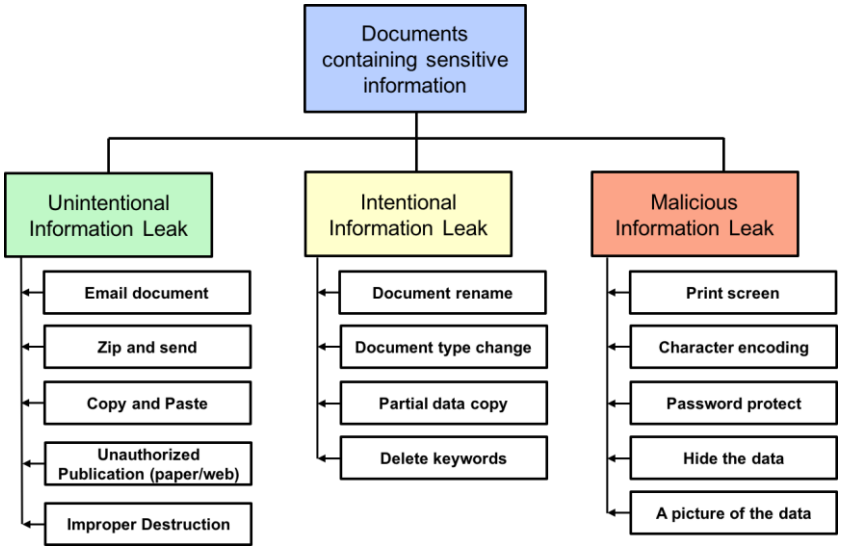


4. การบริหารจัดการด้านความมั่นคงทางคอมพิวเตอร์ภายในองค์กร (Computer Security Management)

4.1. ภัยคุกคามจากบุคคลภายใน (The Insider Threat)

Cyber insider คือผู้ใช้ที่มีสิทธิ์การเข้าถึงข้อมูลแล้วกระทำการที่ไม่ได้รับอนุญาต โดยรูปแบบของ insider ที่เป็นไปได้คือ ลูกจ้างที่ไม่พอใจและคนภายในที่อยู่ในองค์กรก่อการร้ายต่าง โดยจุดมุ่งหมายจะแตกต่างกัน เช่น ขโมยข้อมูล ใส่โปรแกรม malware หรือตั้งใจทำลายระบบโดยตรง นอกจากนี้ผู้ใช้สามารถเป็นช่วยเหลือผู้โจมตีจากภายนอกได้โดยไม่รู้ตัวโดยการให้ข้อมูลหรือให้คนอื่นเข้ามาใน network หรือถูกหลอกให้ลงโปรแกรม virus โดยวิธีการที่เรียกว่า phishing

การรั่วไหลของข้อมูลสำคัญ (information leak) สามารถเกิดขึ้นได้โดยไม่ตั้งใจ (unintentional) โดยตั้งใจ (intentional) และโดยมีจุดประสงค์ร้าย (malicious)



การป้องกันปัญหา insider ทำได้โดยการ

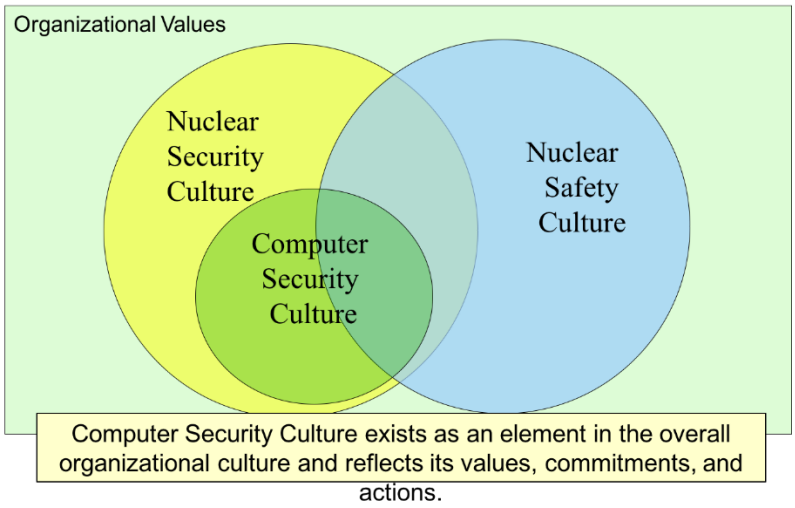
- Screening prior to allow access – ต้องมีการตรวจประวัติของผู้ที่จะได้รับสิทธิ์มาเป็นอย่างดี ว่าไม่มีพฤติกรรมที่ไม่พึงประสงค์
- Observing behaviors after access granted – คอยตรวจตราดูพฤติกรรม ว่ามีลักษณะที่ผิดปกติหรือไม่ หลังจากได้สิทธิ์การใช้งานแล้ว
- Limit opportunities for damage – จำกัดโอกาสการทำผิดและการเข้าถึงข้อมูล

4.2. วัฒนธรรมด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Culture)

เนื่องจากมนุษย์เป็นปัจจัยหลักต่อความมั่นคงทางคอมพิวเตอร์ ดังนั้นองค์กรจะต้องมีวัฒนธรรมด้านความมั่นคง (security culture) เพื่อสนับสนุนให้มาตรการรักษาความปลอดภัยตั้งแต่ระดับบนถึงระดับล่าง ซึ่งการมี security culture จะทำให้เพิ่มระดับความมั่นคง ความปลอดภัย การบริหารจัดการ ประสิทธิภาพการทำงาน ความพอใจของพนักงาน และลดค่าใช้จ่าย

Fundamental Principle โดย IAEA กำหนดให้ security culture เป็นเรื่องที่ต้องได้รับการให้ความสำคัญ และมีเอกสารที่กล่าวถึงหลายฉบับ (NSS No 20, 13, 14, 15, 7) โดยลักษณะสำคัญของ cyber

security culture ประกอบไปด้วย beliefs, attitudes, knowledge, behaviors, competences, management system



การสร้างความตระหนักเรื่อง cyber security สามารถทำได้โดยการจัดอบรม ปิดป้ายประกาศ การประชุมปรึกษาหารือ จัดทำจดหมายข่าว และการแจ้งเตือนต่างๆ เพื่อให้ทุกคนทราบร่วมกัน โดยการจัดอบรมสามารถแบ่งเป็นเนื้อหาทั่วไปสำหรับผู้ใช้ทุกคน เนื้อหาเฉพาะทางเทคนิคสำหรับ administrator, developer, และ engineer และเนื้อหาระดับสูงเพื่อวิเคราะห์ความเสี่ยง ป้องกันภัย และตอบสนองต่อภัยคุกคาม

4.3. การบริหารจัดการบุคลากรด้านความมั่นคง (Human Resource Management and Personnel Security)

การบริหารจัดการบุคลากรด้านความมั่นคง มีส่วนประกอบดังนี้

1. Vetting – ก่อนรับเข้าทำงานต้องมีการตรวจประวัติอย่างละเอียด
2. Conditions of employment – ต้องบังคับให้ผ่านการอบรมให้ตระหนักถึงความสำคัญของความมั่นคงทางคอมพิวเตอร์ และมีการตรวจสอบผลการทำงานอยู่เสมอ
3. Agreement of roles and responsibilities – ต้องมีการกำหนดชัดเจนถึงตำแหน่งและหน้าที่ที่ทุกคนต้องรับผิดชอบ
4. Division or segregation of duties – ต้องมีการตรวจสอบสิทธิ์ที่ทุกคนได้รับว่าตรงกับตำแหน่งหน้าที่ในปัจจุบันหรือไม่ เนื่องจากการย้ายตำแหน่งหรือกลุ่มภายใน
5. Termination procedure – เมื่อมีการให้ออกจากงาน จะต้องปิดสิทธิ์การใช้งานของบุคคลนั้นโดยทันที

นอกจากนี้ ถ้ามีส่วนเกี่ยวข้องกับผู้อื่นเข้ามาในระบบ จะต้องระมัดระวัง มีการประเมินความเสี่ยง และบริหารจัดการการเข้าถึงข้อมูลให้ถูกต้อง

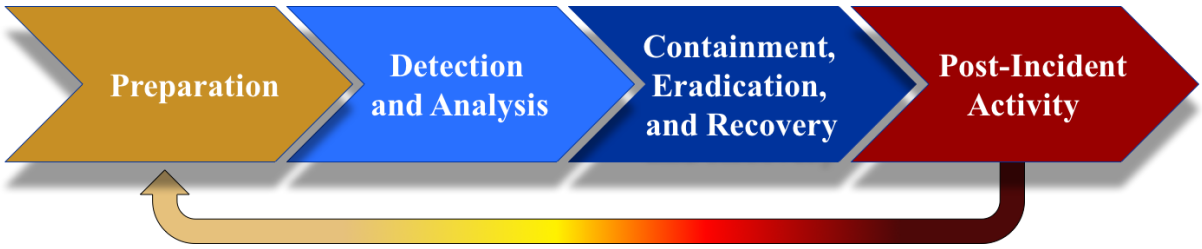
5. การตอบสนองต่อเหตุการณ์ด้านความมั่นคงทางคอมพิวเตอร์ (Computer Security Incident Response)

การตอบสนองต่อเหตุการณ์ (incident response) คือความสามารถในการตรวจจับและแก้ปัญหาที่อาจมีผลกับบุคคล กระบวนการ เทคโนโลยี และสถานประกอบการ ซึ่งมีจุดมุ่งหมายในการวางแผนการ

ตอบสนองเพื่อลดเวลาหยุด (downtime) ตรวจสอบว่าเกิดอะไรขึ้น ป้องกันการโจมตีในอนาคต และจับผู้กระทำผิด

ผู้มีส่วนได้ส่วนเสียในการตอบสนองต่อเหตุการณ์ แบ่งออกเป็น 3 กลุ่ม

1. State
2. Competent Authority
3. Technical Support Organization
4. Nuclear Facility (Licensee)



วงจรการตอบสนองต่อเหตุการณ์ (incident response life cycle) ประกอบไปด้วย

1. Preparation
    a. จัดตั้งทีมตอบสนองต่อเหตุการณ์ (security incident response team) ประกอบไปด้วย ผู้นำทีม วิศวกร ผู้เชี่ยวชาญด้าน security ผู้ใช้งาน ฝ่ายประชาสัมพันธ์ และเจ้าหน้าที่ผู้มีความรู้ในด้านต่างๆ
    b. กำหนดกระบวนการการตอบสนองต่อเหตุการณ์ โดยแบ่งออกตามความน่าจะเป็นและผลกระทบที่อาจเกิดขึ้น และวางแผนการตอบสนองต่อเหตุการณ์นั้นๆ
2. Detection and Analysis
    a. ตรวจจับเหตุการณ์ผิดปกติ ที่อาจเกิดจากการโจมตีทางไซเบอร์ ประกอบไปด้วยการเช็ค log file, การได้รับแจ้งเตือนจาก antivirus, มีการติดต่อกับ IP ข้างนอก, มีการเปลี่ยนแปลง config, มีการใช้ CPU มากเกินไป
    b. มีการทำการวิเคราะห์ให้ทราบถึงขอบเขตของเหตุการณ์ เพื่อป้องกันความเสียหายที่มากขึ้น และเพื่อจะหาว่าผู้ทำการโจมตีมาจากที่ไหน
3. Containment, Eradication, and Recovery
    a. ทำการป้องกันความเสียหาย โดยการควบคุมไม่ให้โจมตีเข้าไปในส่วนที่ลึกขึ้น โดยมี criteria และขั้นตอนที่ชัดเจน แต่ต้องระวังไม่ให้มีความเสียหายถ้าไปควบคุมอย่างไม่ถูกวิธี
    b. ทำการกำจัดส่วนที่ถูกโจมตี หลังจากเข้าใจขอบเขตของการโจมตีทั้งหมด
    c. จากนั้นดำเนินการปรับระบบทุกอย่างให้กลับมาอยู่ในสภาพปกติ
4. Post-Incident Activity
    a. นำข้อมูลที่ได้จากการถูกโจมตีมาวิเคราะห์และปรับปรุงป้องกันไม่ให้ถูกโจมตีในแบบเดียวกันได้อีกในอนาคต
    b. แบ่งปันข้อมูลที่ได้ให้ทุกคนทราบและให้ผู้อื่นได้รู้

บทสรุป

การดำเนินการหลักเพื่อส่งเสริมความมั่นคงทางคอมพิวเตอร์ในงานด้านนิวเคลียร์แลรังสี มีดังต่อไปนี้ (1) ทำการวิเคราะห์ด้านความมั่นคงทางคอมพิวเตอร์ภายในหน่วยงาน และมีการดำเนินการปรับปรุงการป้องกันข้อมูลที่สำคัญให้เป็นไปตามมาตรฐานสากล พร้อมทั้งฝึกอบรมบุคลากรภายในหน่วยงาน ให้ตระหนักถึงความสำคัญและช่วยกันดูแลไม่ให้เกิดการถูกโจมตีทางไซเบอร์ (2) จัดทำกฎระเบียบประกอบการขออนุญาตและให้คำแนะนำเพิ่มเติม ในการบริหารจัดการด้านความมั่นคงทางคอมพิวเตอร์สำหรับสถานประกอบการทางนิวเคลียร์ เพื่อที่ส่งเสริมให้ผู้ประกอบการทราบถึงภัยอันตรายที่อาจเกิดขึ้น และดำเนินการสร้างมาตรการป้องกันให้เพียงพอตามความจำเป็น (3) พัฒนาหลักสูตรและเนื้อหาการสอนทางด้านความมั่นคงทางคอมพิวเตอร์เพื่อเป็นส่วนประกอบหนึ่งของโครงการพัฒนาความมั่นคงทางนิวเคลียร์ โดยให้ผู้เข้าร่วมได้ความรู้พื้นฐานในเรื่องของคำแนะนำจาก IAEA และมาตรฐานสากลในการจัดการด้านความมั่นคงทางคอมพิวเตอร์ และตระหนักถึงความสำคัญของความมั่นคงทางคอมพิวเตอร์ในระบอบความมั่นคงทางนิวเคลียร์

เอกสารอ้างอิง

เอกสารประกอบการฝึกอบรม International Regional Workshop on the Development of National Training Programmes in Computer Security ณ เมือง โตไก ประเทศ ญี่ปุ่น ตั้งแต่วันที่ 27 มิถุนายน 2559 ถึง 1 กรกฎาคม 2559