สรุปภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security

โดยอาจารย์ปริญญา หอมเอนก

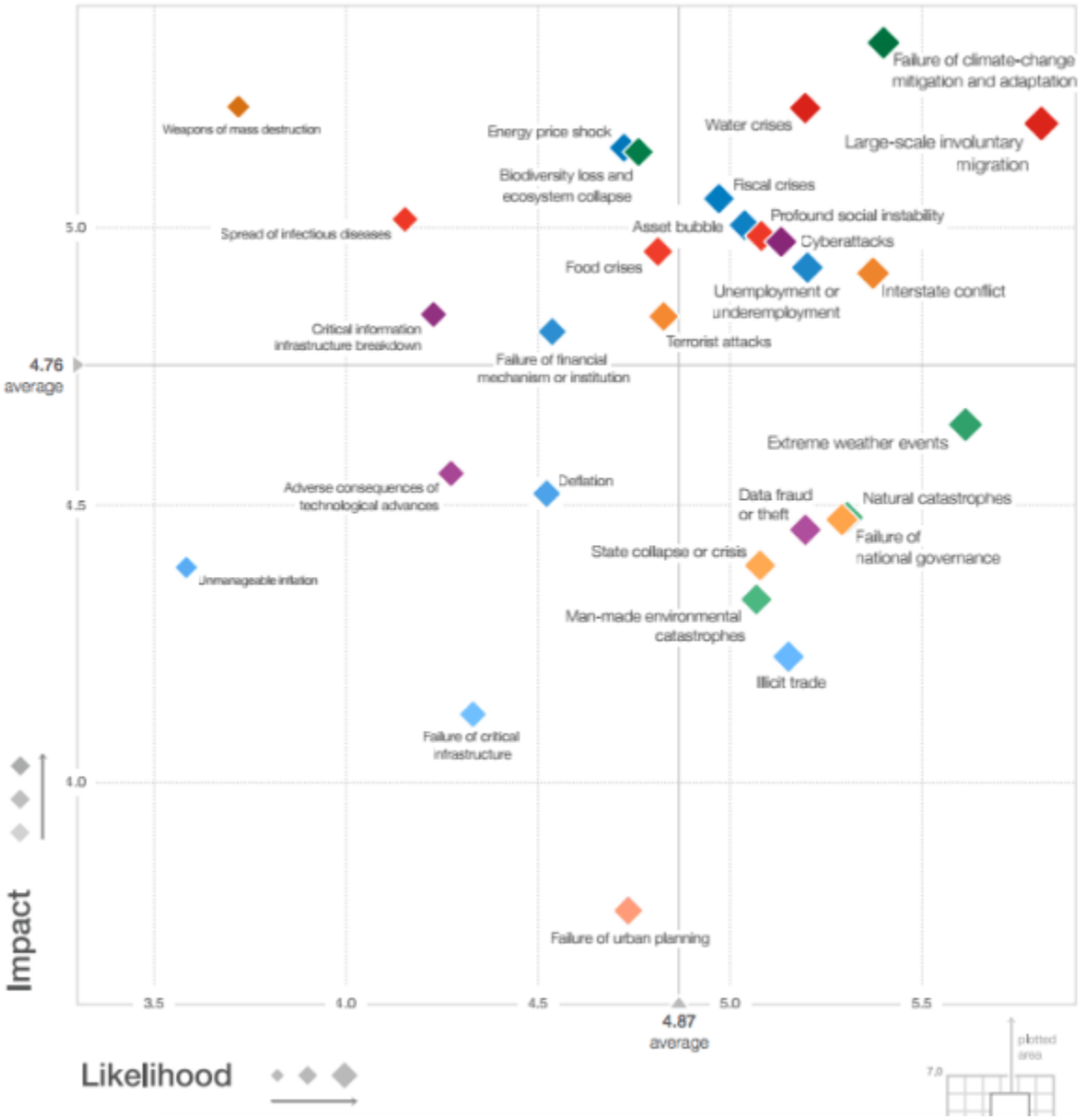
อาจารย์ปริญญา หอมเอนก ผู้ก่อตั้งบริษัท ACIS Professional Center และผู้บริหารบริษัท Cybertron เริ่มเซสชันงาน **CDIC 2016** ด้วยการสรุปแนวโน้มภัยคุกคามและทิศทางด้าน Cyber Security ในปี 2016 – 2018 ไม่ว่าจะเป็นเรื่อง Block Chain, Fin Tech และ Cyber Warfare พร้อมแนะนำเครื่องมือและวิธีการเพื่อเสริมความแข็งแกร่งให้กับระบบรักษาความมั่นคงปลอดภัยในองค์กร

"ปัจจุบันนี้เราเน้นพัฒนาและประยุกต์ใช้แอพพลิเคชันให้มีประสิทธิภาพมากยิ่งขึ้น แต่ต้องไม่ลืมเรื่อง Security และ Privacy ของการใช้แอพพลิเคชันอย่างเด็ดขาด" — อาจารย์ปริญญากล่าว

การก่อการร้ายไซเบอร์ ภัยคุกคามที่ต้องจับตามอง

รายงาน The Global Risks Report ประจำปี 2016 โดย World Economic Forum จัดอันดับให้การก่อการร้ายไซเบอร์เป็นหนึ่งในภัยคุกคามที่มีความรุนแรงเกินกว่าค่าเฉลี่ยของภัยคุกคามรูปแบบต่างๆ ทั้งหมด ซึ่งปัจจุบันนี้หลายประเทศทั่วโลกได้จัดกองทัพไซเบอร์เป็น 1 ใน 5 โดเมนสำหรับป้องกันประเทศนอกจากทัพบก เรือ

อากาศ นาวิกโยธิน หน่วยงานรัฐควรให้การสนับสนุนและสร้างบุคลากรเพื่อให้สามารถปกป้องอธิปไตยจากภัยก่อการร้ายไซเบอร์ได้



Fin Tech VS. Blockchain

เมื่อพูดถึง Fin Tech หลายท่านมักจะนึกถึง Blockchain แต่อันที่จริงแล้วไม่จำเป็นเสมอไป ด้วยนิยามของ Fin Tech (หรือ Financial Technology) คือ เป็นเทคโนโลยีที่ช่วยให้บริการด้านการเงินต่างๆ มีประสิทธิภาพดียิ่งขึ้น ซึ่งเริ่มต้นตั้งแต่ตู้ ATM บัตรเครดิต ไปจนถึงระบบ SWIFT ซึ่ง Blockchain เองก็อาจกล่าวได้ว่าเป็นเทคโนโลยีล่าสุดของ Fin Tech ที่เป็นที่น่าสนใจและน่าจับตามองอย่างมากในปัจจุบัน

อย่างไรก็ตามภัยคุกคามไซเบอร์ก็มีการพัฒนาเพื่อให้สามารถโจมตีระบบเหล่านี้ได้เช่นกัน ยกตัวอย่างเช่น **Skimer** ซึ่งเป็นมัลแวร์บนตู้ ATM ตัวแรกของโลก ซึ่งแอบอ่านข้อมูลบัตร ATM จากซอฟต์แวร์ภายในเครื่อง แล้วนำไปสร้างบัตรปลอมเพื่อกดเงินออกมาแทน หรือการโจมตีแบบ **ATM Jackpoting** ถึงแม้ว่า ATM จะเปลี่ยนจากการใช้แถบแม่เหล็กมาใช้เป็น Chip & Pin ซึ่งมีความมั่นคงปลอดภัยมากกว่า แฮ็คเกอร์ก็พัฒนาเทคนิคการโจมตีเพื่อให้สามารถแฮ็คข้อมูลและขโมยเงินได้แล้วเช่นกัน แต่การโจมตีเหล่านั้นยังต้องใช้เงื่อนไขที่ค่อนข้างเยอะและประสบความสำเร็จในห้องแล็ปเท่านั้น

Blockchain นวัตกรรมเปลี่ยนโลก

Blockchain เป็นเทคโนโลยีใหม่ที่กำลังเป็นที่กล่าวขานในปัจจุบัน เนื่องจากช่วยให้ผู้ใช้สามารถทำธุรกรรมออนไลน์ เช่น โอนเงิน ส่งไฟล์ MP3 เทรดหุ้น หรือแม้แต่โหวตเสียงเลือกตั้งได้โดยไม่จำเป็นต้องมีคนกลาง และเป็นระบบที่มีการออกแบบอัลกอริธึมให้มีความมั่นคงปลอดภัยสูง Blockchain ที่โด่งดังที่สุดในปัจจุบันคงหนีไม่พ้น Bitcoin ซึ่งเป็น Digital Currency สำหรับโอนเงินและชำระเงิน ซึ่งปัจจุบันนี้ร้านค้าออนไลน์หลายแห่ง เช่น Payay, Ebay, Domino Pizza รวมไปถึงหน่วยงานรัฐบาลบางประเทศทำการยอมรับแล้วว่าสามารถใช้ทำธุรกรรมได้จริง ธนาคารชื่อดังแห่งหนึ่งในไทยเองก็ยอมรับการใช้ Ripple (Digital Currency ประเภทหนึ่ง) ให้สามารถทำธุรกรรมออนไลน์ได้เช่นกัน

“Blockchain เปรียบเสมือนเป็น Swiss Army Knife ที่มีฟังก์ชันการใช้งานอันหลากหลาย ทุกคนสามารถนำไปใช้ให้เกิดประโยชน์ได้ตามจินตนาการ เรียกได้ว่าเป็นการปฏิวัติระบบอินเทอร์เน็ตให้เข้าสู่ยุคใหม่ ผมบอกได้เลยว่า Blockchain มาแน่นอน แค่ว่าเมื่อไหร่เท่านั้น” — อาจารย์ปริญญาให้ความเห็น

ถึงแม้ว่า Blockchain จะมีแนวคิดด้านความมั่นคงปลอดภัยที่แข็งแกร่ง แต่ไม่มีระบบใดที่สมบูรณ์แบบ 100% ในอดีต Core Technology ของ Bitcoin เคยทำงานผิดพลาดถึง 2 ครั้ง ได้แก่ กรณี Block 74638 เกิด Value Overflow และในเดือนมีนาคมปี 2013 ก็เกิดเหตุการณ์ Bitcoin Fork หรือก็คือ Node ของ Bitcoin แยกออกเป็น 2 ทาง ซึ่งเป็นเส้นทางที่มีการคำนวณแล้วว่าถูกต้อง สาเหตุมาจากปัญหาระดับ Database-level ซึ่งสุดท้ายก็จำเป็นต้องตัดเส้นทางหนึ่งทิ้งไป

สรุปแนวโน้มภัยคุกคามและทิศทางด้านความมั่นคงปลอดภัยในปี 2016 – 2018

- Cyber Security ไม่ใช่เรื่องเฉพาะฝ่าย IT อีกต่อไป หากเป็นเรื่องที่ต้องนำเข้าที่ประชุม **“บอร์ดบริหาร”** ขององค์กร
- Microsoft ได้นำหลักการของ NIST Cybersecurity Framework มาใช้ใน Microsoft CDOC ได้แก่ Protect, Detect และ Respond
- Cyber Threat Intelligence เป็นการเปลี่ยนวิธีารบริหารจัดการความมั่นคงปลอดภัยจาก **“Reactive”** เป็น **“Proactive”**

- แฮ็คเกอร์จะมุ่งหน้าดจมตีไปยังเป้าหมายเฉพาะ แต่มีผลกระทบและสร้างความเสียหายสูงต่อองค์กร
- การโจมตีของแฮ็คเกอร์จะมีลักษณะต่อเนื่องและฝังตัวเป็นระยะเวลานานกว่าองค์กรจะตรวจจับได้ว่าถูกแฮ็ค (Advanced Persistent Threats)
- แฮ็คเกอร์พุ่งเป้าโจมตีองค์กรขนาดใหญ่ และมีรัฐบาลให้การสนับสนุนอยู่เบื้องหลัง (State-sponsored Attack)
- องค์กรจำเป็นต้องมีความสามารถในการตามล่าและติดตามแฮ็คเกอร์ในโลกจริงที่ไม่ใช่เพียงโลกไซเบอร์

"ปัจจุบันนี้แฮ็คเกอร์ระดับประเทศเขาไม่แฮ็คระบบหรือปล่อยมัลแวร์กันแล้ว แต่ใช้วิธีฝัง Backdoor มากับอุปกรณ์ IoT เช่น CCTV, IP Camera หรือ Router ตั้งแต่แรกแทน ส่งผลให้แฮ็คเกอร์สามารถเข้าโจมตีระบบผ่านอุปกรณ์หรือสร้างกองทัพซอมบี้ไว้โจมตี DDoS แบบที่ปรากฏในข่าวล่าสุดได้ตามต้องการทันที" — อาจารย์ปริญญาอธิบาย

20

Awareness Training ไม่เพียงพอ ต้อง Cyber Drill

หลายองค์กรมีการจัดอบรมพนักงานเพื่อให้ตระหนักถึงภัยคุกคามไซเบอร์ อย่างไรก็ตาม การอบรมเหล่านั้นมักใช้ได้ผลเพียง 1 – 2 สัปดาห์เท่านั้น หลังจากนั้นพนักงานก็จะกลับมาตกเป็นเหยื่อของแฮ็คเกอร์ใหม่ แสดงให้เห็นว่าการจัดอบรมเพียงอย่างเดียวไม่เพียงพอ จำเป็นต้องมีการซ้อมรับมือกับสถานการณ์จริง หรือที่เรียกว่า Cyber Drill (เช่นเดียวกับการซ้อมหนีไฟ) เพื่อให้พนักงานในองค์กรคุ้นเคยกับภัยคุกคามไซเบอร์ต่างๆ เช่น Phishing และ Ransomware ส่งผลให้สามารถตอบสนองต่อเหตุการณ์เมื่อเกิดขึ้นจริงได้อย่างถูกต้องและรวดเร็ว บริษัท IT ยักษ์ใหญ่หลายแห่ง เช่น Google, Microsoft และ Cisco ก็มีการฝึกฝนพนักงานด้วยวิธีนี้

ผู้ที่สนใจสามารถอ่านรายละเอียดเนื้อหาทั้งหมดที่อาจารย์ปริญญานำเสนอได้ที่ https://www.goo.gl/avJ5TJ