ตกลง(วงการ)หมอพร้อมหรือไม่พร้อม สำหรับภัยคุกคาม cybersecurity ในยุคนี้? -- ความเห็นส่วนตัวจากหมอไอทีคนหนึ่ง

นพ.นวนรรน ธีระอัมพรพันธุ์

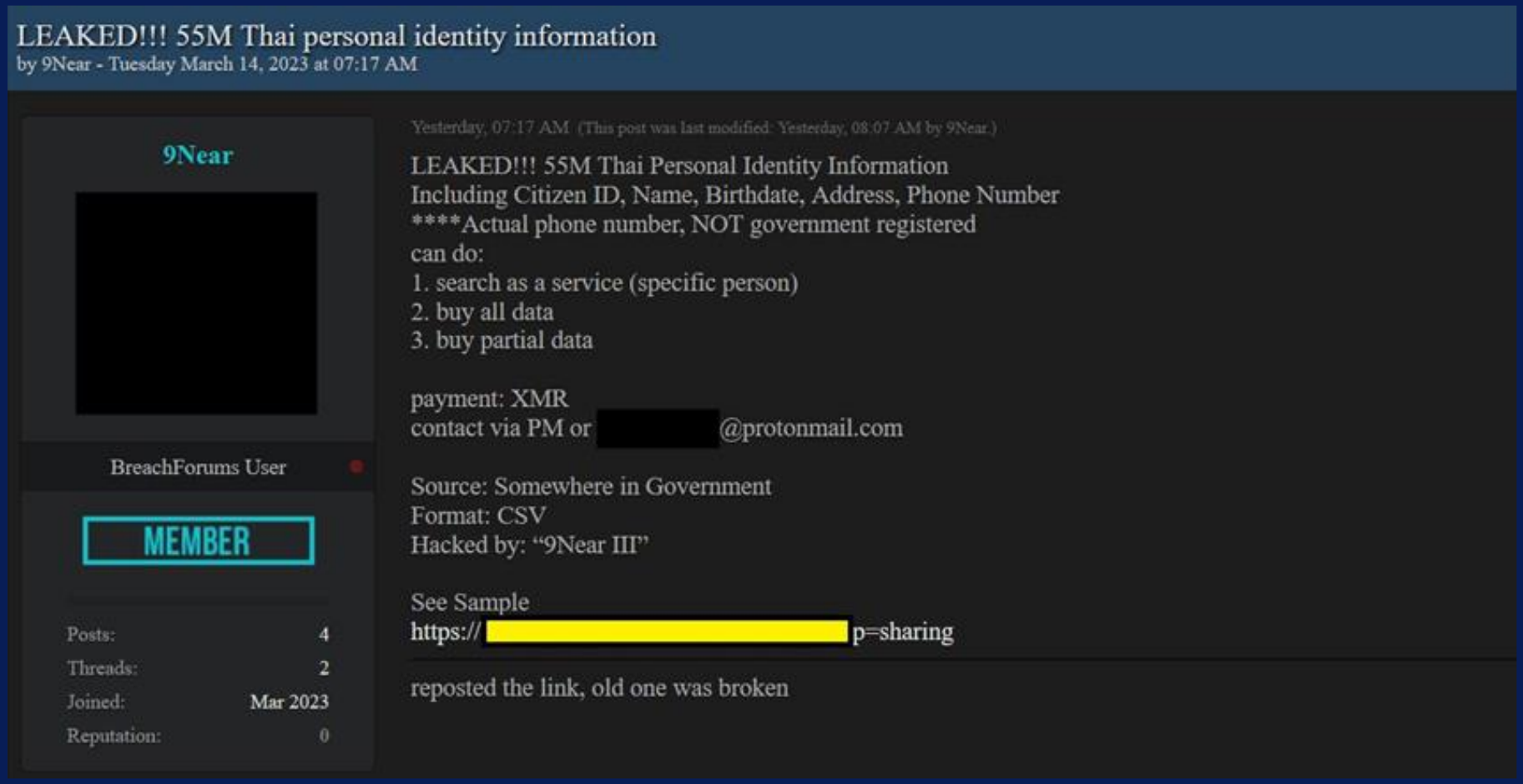
คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล

10 มิถุนายน 2566

Disclaimer:

1. เป็นความเห็นทางวิชาการส่วนบุคคล ไม่ผูกพันการทำหน้าที่ในบทบาทใดในปัจจุบันหรืออนาคต
2. ข้อมูลบางส่วนมาจากการทำหน้าที่ในคณะแพทยศาสตร์โรงพยาบาลรามาธิบดี มหาวิทยาลัยมหิดล และในบทบาทนักวิชาการด้าน Health Information Privacy
3. การนำเสนอไม่ได้มีการเปิดเผยความลับที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรายใดมีการแจ้งเหตุมายังหน่วยงานกำกับหรือผู้มีอำนาจตามกฎหมาย หรือผู้นำเสนอ หรือที่หน่วยงานกำกับหรือผู้มีอำนาจตามกฎหมาย หรือผู้นำเสนอ ได้มาและมีหน้าที่รักษาข้อมูลนั้นไว้เป็นความลับตามกฎหมาย
4. การกล่าวถึงระบบใดหรือหน่วยงานใด ไม่ได้เป็นการใส่ความหรือกล่าวหาว่าระบบนั้นหรือหน่วยงานนั้นกระทำผิดหรือมีความบกพร่องแต่อย่างใด เป็นเพียงการแสดงความคิดเห็นหรือข้อความโดยสุจริตเพื่อติชมด้วยความเป็นธรรม อันเป็นวิสัยของประชาชนย่อมกระทำ

The 9Near Incident (14 March 2023)



LEAKED!!! 55M Thai personal identity information
by 9Near - Tuesday March 14, 2023 at 07:17 AM

9Near

BreachForums User

MEMBER

Posts:	4
Threads:	2
Joined:	Mar 2023
Reputation:	0

Yesterday, 07:17 AM (This post was last modified: Yesterday, 08:07 AM by 9Near.)

LEAKED!!! 55M Thai Personal Identity Information
Including Citizen ID, Name, Birthdate, Address, Phone Number
****Actual phone number, NOT government registered
can do:
1. search as a service (specific person)
2. buy all data
3. buy partial data

payment: XMR
contact via PM or [redacted]@protonmail.com

Source: Somewhere in Government
Format: CSV
Hacked by: "9Near III"

See Sample
https://[redacted]p=sharing

reposted the link, old one was broken

https://breached.vc/ (Now Taken Down)

The 9Near Incident (17 March 2023)

“แฮกเกอร์”ประกาศขายข้อมูลส่วนตัวคนไทย 55 ล้านรายชื่อ อ้างได้มาจากหน่วยงานรัฐ

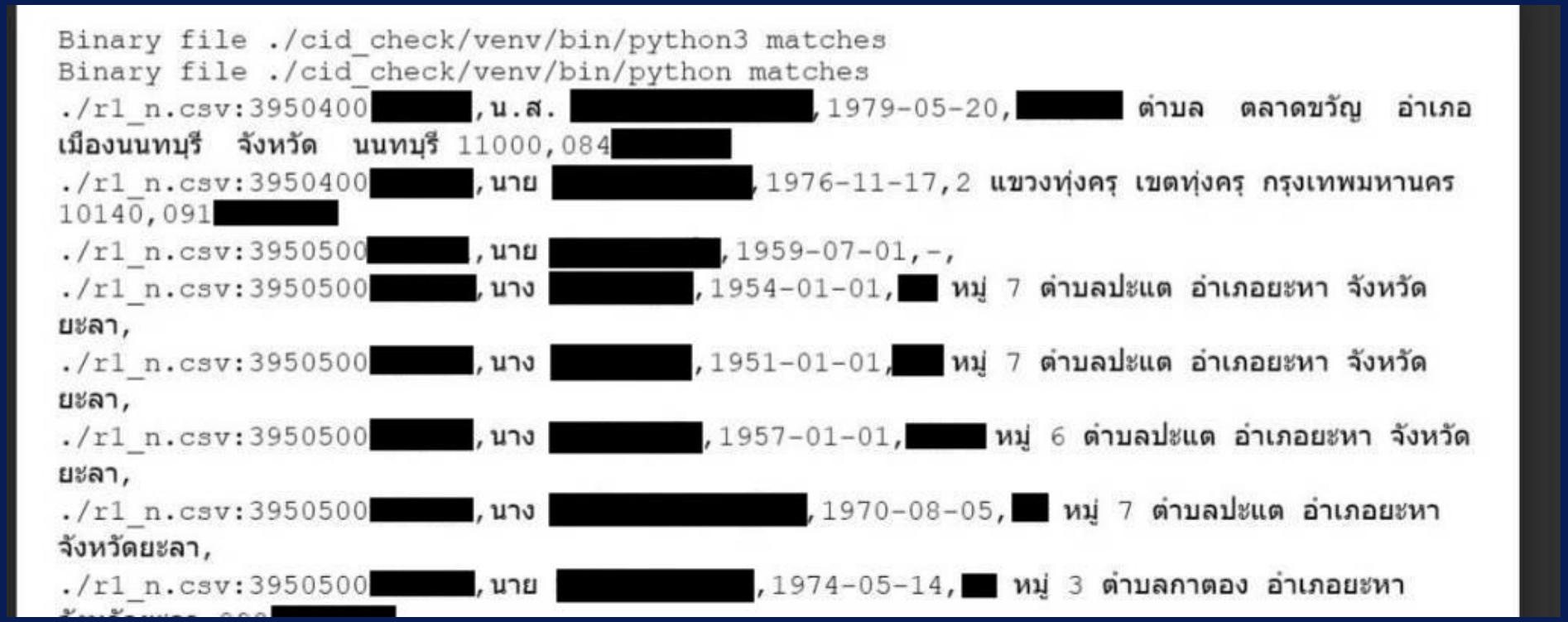
Khaosod

อัพเดต 17 มี.ค. เวลา 16.35 น. • เผยแพร่ 17 มี.ค. เวลา 12.50 น.

ติดตาม

https://today.line.me/th/v2/article/60rzN9B

The 9Near Incident (17 March 2023)



```
Binary file ./cid_check/venv/bin/python3 matches
Binary file ./cid_check/venv/bin/python matches
./r1_n.csv:3950400[redacted],น.ส. [redacted],1979-05-20,[redacted] ตำบล ตลาดขวัญ อำเภอ
เมืองนนทบุรี จังหวัด นนทบุรี 11000,084[redacted]
./r1_n.csv:3950400[redacted],นาย [redacted],1976-11-17,2 แขวงทุ่งครุ เขตทุ่งครุ กรุงเทพมหานคร
10140,091[redacted]
./r1_n.csv:3950500[redacted],นาย [redacted],1959-07-01,-,
./r1_n.csv:3950500[redacted],นาง [redacted],1954-01-01,[redacted] หมู่ 7 ตำบลปะแต อำเภอยะหา จังหวัด
ยะลา,
./r1_n.csv:3950500[redacted],นาง [redacted],1951-01-01,[redacted] หมู่ 7 ตำบลปะแต อำเภอยะหา จังหวัด
ยะลา,
./r1_n.csv:3950500[redacted],นาง [redacted],1957-01-01,[redacted] หมู่ 6 ตำบลปะแต อำเภอยะหา จังหวัด
ยะลา,
./r1_n.csv:3950500[redacted],นาง [redacted],1970-08-05,[redacted] หมู่ 7 ตำบลปะแต อำเภอยะหา
จังหวัดยะลา,
./r1_n.csv:3950500[redacted],นาย [redacted],1974-05-14,[redacted] หมู่ 3 ตำบลกาตอง อำเภอยะหา
```

รายชื่อและข้อมูลส่วนบุคคลของบุคคลที่ถูกละเมิด (บางส่วน) ตามที่เป็นข่าวเมื่อ 17 มีนาคม 2566
(data masking done for this presentation)

The 9Near Incident (18 March 2023)

ชี้พบพิรุธ “แฮกเกอร์” ประกาศขาย 55 ล้านข้อมูลคนไทย หน่วยงานมั่นคงเร่งตรวจสอบ

เดลินิวส์

อัพเดต 18 มี.ค. เวลา 19.04 น. • เผยแพร่ 18 มี.ค. เวลา 09.46 น. • เดลินิวส์

ติดตาม

https://today.line.me/th/v2/article/9mrr0ae

The 9Near Incident (18 March 2023)

จากกรณีที่มีกระแสบนโลกออนไลน์ ที่มีแฮกเกอร์ ที่ใช้นามแฝงว่า “9Near” ได้โพสต์ประกาศขายข้อมูลในเว็บ BreachForum ซึ่งเป็นเว็บบอร์ดที่ใช้สำหรับซื้อขายข้อมูลส่วนบุคคล ที่หลุดออกมาจากหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนในหลายประเทศ

โดยระบุว่า มี 55 ล้านข้อมูลรายชื่อคนไทย มีรายละเอียดทั้งชื่อ นามสกุล ที่อยู่ วันเกิด เลขประจำตัวประชาชน เบอร์โทรศัพท์ ที่เป็นเบอร์ที่ใช้งานจริง ส่งผลให้เกิดกระแสวิพากวิจารณ์เรื่องนี้จำนวนมากนั้น

https://today.line.me/th/v2/article/9mrr0ae

The 9Near Incident (18 March 2023)

แหล่งข่าวจากหน่วยงานความมั่นคงของไทย เปิดเผยกับ "เดลินิวส์" ว่า หลังมีการประกาศขายทาง เจ้าหน้าที่ ได้เร่งตรวจสอบข้อมูล และลองดาวน์โหลดข้อมูลตัวอย่างมา พบว่ามีข้อมูลส่วนบุคคล ประมาณ 200 คน ซึ่งเมื่อนำมาวิเคราะห์ เหมือนข้อมูลหลอกประกาศขาย โดยตอนแรก แฮกเกอร์รายนี้ ได้นำไปประกาศขายยังอีกเว็บแต่ถูกลบไป จากนั้นจึงนำมาประกาศใหม่อีกรอบในอีกเว็บ เมื่อสมัครแล้วรีบลงประกาศขายทันที จึงดูพฤติกรรมแปลกว่า เป็นการหลอกขายหรือไม่ ซึ่งปัจจุบันก็มีการหลอกขายข้อมูลแบบนี้อยู่ตลอด

“ตอนนี้หน่วยงานที่เกี่ยวข้องกำลังร่วมมือกันตรวจสอบ เพราะวิธีการแชร์ก็แปลกเป็นการใช้กูเกิลไดรฟ์ แจก ซึ่งปกติแฮกเกอร์จะไม่ใช้แบบนี้ และปกติเมื่อมีการแฮกข้อมูลได้ถึง 55 ล้านคนจะมีการแจกตัวอย่างข้อมูลที่มากกว่านี้ เพื่อสร้างความเชื่อมั่นให้คนที่ต้องการซื้อ เหมือนเช่นกรณีที่มีการแฮกรายชื่อผู้ป่วยของโรงพยาบาลที่เพชรบูรณ์ในอดีต ซึ่งก็มีระบุว่า 2 หมื่นรายชื่อ และมีการแจกให้ข้อมูลตัวอย่างที่มากว่านี้ แต่กรณีนี้อ้างว่ามี 55 ล้านรายชื่อ ซึ่งเป็นจำนวนเกือบทั้งประเทศ แต่ให้ข้อมูลเพียง 200 รายชื่อเท่านั้น ปกติต้องมีการแจกข้อมูลที่มากกว่านี้ เพื่อสร้างความน่าเชื่อถือ ชวนให้คนอยากซื้อ และว่าไม่ได้หลอก”

สำหรับแฮกเกอร์รายนี้ จะเป็นคนไทยหรือต่างประเทศนั้น จากการวิเคราะห์ชื่อ หรือนามแฝง ใช้คำที่พ้องกับพรรคการเมือง ที่มีการเล่นคำ จึงเชื่อว่าแฮกเกอร์รายนี้อาจจะเข้าใจภาษาไทย อย่างไรก็ตาม ยังมีข้อสงสัยที่ต้องเร่งตรวจสอบอยู่ โดยหน่วยงานที่เกี่ยวข้องจะพยายามตรวจสอบให้ได้ข้อมูลเร็วที่สุด

https://today.line.me/th/v2/article/9mrr0ae

The 9Near Incident (23 March 2023)

สธ.ยันระบบ หมอพร้อม ปลอดภัย หลังกระแสข่าวข้อมูลคนไทยถูกแฮก 55 ล้านคน

ชมรมแพทย์ชนบทจี้ สธ.ให้ข้อมูลหลังมีข่าวข้อมูลส่วนตัวคนไทย 55 ล้านคนถูกแฮกเกอร์ประกาศขาย คาดมาจาก หมอพร้อม ล่าสุดผู้ช่วยรัฐมนตรี สธ. ชี้ตรวจสอบแล้ว ไม่ใช่ ระบบ หมอพร้อม มีข้อมูลเพียง 30 ล้าน จับคู่ข้อมูลที่อ้างถูกแฮกไม่ตรงกับในระบบที่มี

เมื่อวันที่ 23 มีนาคม ชมรมแพทย์ชนบท โพสต์ข้อมูลระบุว่า ข้อมูลส่วนตัวคนไทย 55 ล้านคนถูกแฮกเกอร์ประกาศขาย คาดว่าอาจจะมาจาก “หมอพร้อม” จริงไหม โดยระบุว่า เป็นเรื่องใหญ่มากเมื่อข้อมูลคนไทยค่อนประเทศถูกแฮกไปแล้ว ฐานข้อมูลขนาดนี้มีไม่กี่รายในประเทศไทย หนึ่งในนั่นคือ หมอพร้อม ที่กระทรวงสาธารณสุขดูแลอยู่ และใช้เป็นฐานในการลงทะเบียนวัคซีนโควิด โดยอ้างอิงข้อมูลว่า มาจากสื่อประชาไท

หมอพร้อม ปลอดภัยไร้ถูกแฮก

https://www.hfocus.org/content/2023/03/27313

The 9Near Incident (29 March 2023)

9Near - Hacktivist

****1990 Bangkok Sensored....**

!! Download !!

Sponsored By...

AND...

นาย ปริญญา หอมเอนก [redacted]

ตำบล [redacted] **อำเภอ** [redacted] **จังหวัด** [redacted]

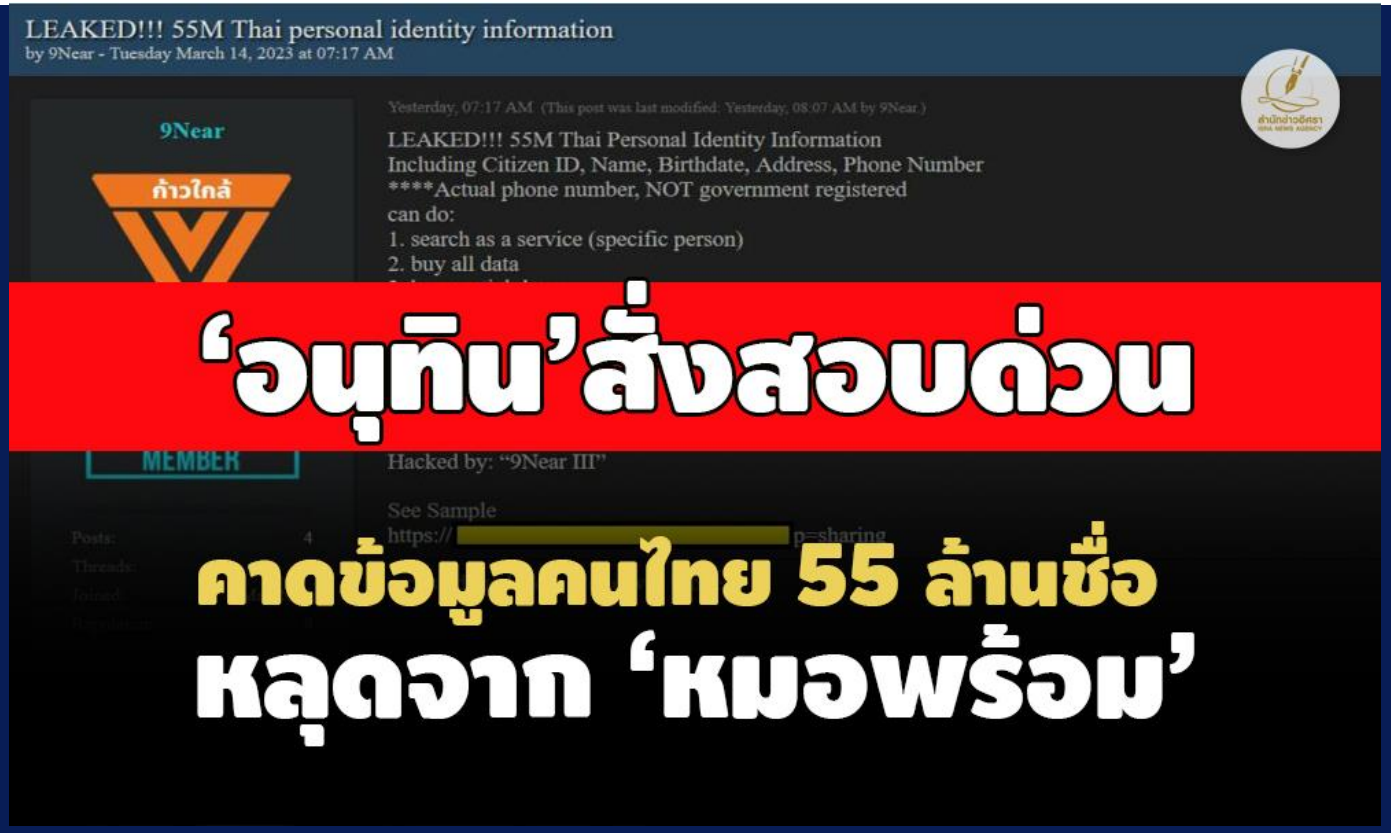
https://9near.org/ (Now Blocked)

The 9Near Incident (30 March 2023)

หน้าแรก / ISRANEWS / ข่าว

DESจัดการเอง! 'อนุทิน' สั่งสอบแฮกเกอร์ขู่แฉข้อมูลไทย 55 ล้านชื่อ-คนในสธ.ชี้เป้าหมอพร้อม

วันพฤหัสบดี ที่ 30 มีนาคม 2566 เวลา 21:21 น. isranews HITS 6688 views



https://www.isranews.org/article/isranews-news/117448-inves0999-3.html

The 9Near Incident (2 April 2023)

9Near - Hacktivist

To all:
Good news…
"OPERATION STOPPED" as our sponsor conflict.
As we don't wanna hurt all of you and also we disagree with this dirty political operation as their plan went too dirty. So we have no reason to continue making this privacy disaster.
At least these few days, we see the great movement how government should concern on citizen security and privacy.

Fact:
We didn't buy data from any authority.
We are not the call center or scammer shit.
We've never sold full data to any as it's still our negotiation power.
Our data is for the movement, not for the money

---

https://9near.org/ (Now Blocked)

The 9Near Incident (2 April 2023)

To our (Anonymous?) sponsor:
Bro, Per our latest talk, As you actual plan is not our purpose. It is for yourself not the people. You see the impact we made on your political shit? You think we met anonymously then we talk anonymously? We know who exactly you are and what side you are in. Also, we think Thai people know. Same countdown, finish the negotiation before something happens.

To all those hunter:
We cloudy scripted to publish the data every 7 days for 10 years. We have destroyed the shell key with only api access. Only us to reset the script via API to stop the privacy disaster. You know the impact.
You catch one, we start the script. Stay in your space
Don't wake us up, else we will be back
Our lovely friends, thanks for joining us we stay in the group

---

Join our community: Telegram

https://9near.org/ (Now Blocked)

Preliminary Data Assessment

- Sample data: 1990x.txt
- 90,000+ records (บาง records มี new line characters = 2 lines)
- Data elements: เลขประจำตัวประชาชน ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ (บาง elements มี data masking)
- All records: birthYear==1990 && address== กรุงเทพมหานคร

https://breached.vc/ (Now Taken Down)

Preliminary Data Assessment

- บาง record มีที่อยู่ที่มีบ้านเลขที่ บาง record มีข้อมูลระดับตำบลขึ้นไป หรืออำเภอขึ้นไป แสดงว่าข้อมูลไม่ clean น่าจะมีประเด็นด้านคุณภาพของข้อมูล (data quality) อาจมีที่มาจากหลายแหล่ง และอาจมีข้อมูลที่ไม่ถูกต้องปะปนอยู่ได้ (data accuracy issues)
- มีหมายเลขโทรศัพท์ในไฟล์ sample data จึงอาจไม่ใช่ข้อมูลจากระบบทะเบียนราษฎรโดยตรงเพียงอย่างเดียว
- บาง record ใน sample data จะถูกปัดเป็น 2 บรรทัด เท่าที่กวาดตาดู มักจะเป็น record ที่ไม่มีหมายเลขโทรศัพท์ ทำให้การปกปิด (mask) หมายเลขโทรศัพท์ด้วย “XXXXXX-” ถูกปัดเป็นบรรทัดต่อไป ซึ่งอาจเป็นข้อผิดพลาด (bug) ของกระบวนการ transform data ของผู้กระทำผิดเอง เป็นไปได้ว่าตอนเขียน code เพื่อ mask data อาจ handle logic กรณีไม่มีหมายเลขโทรศัพท์ผิดพลาด ทำให้ “XXXXXX-” ถูก add หลังอักขระ new line character แทนที่จะถูก add ก่อนอักขระ new line character ดังกล่าว ซึ่งสะท้อนว่าผู้กระทำผิดอาจไม่ใช่มืออาชีพนักหรืออาจไม่ได้มีความละเอียดรอบคอบเต็มที่

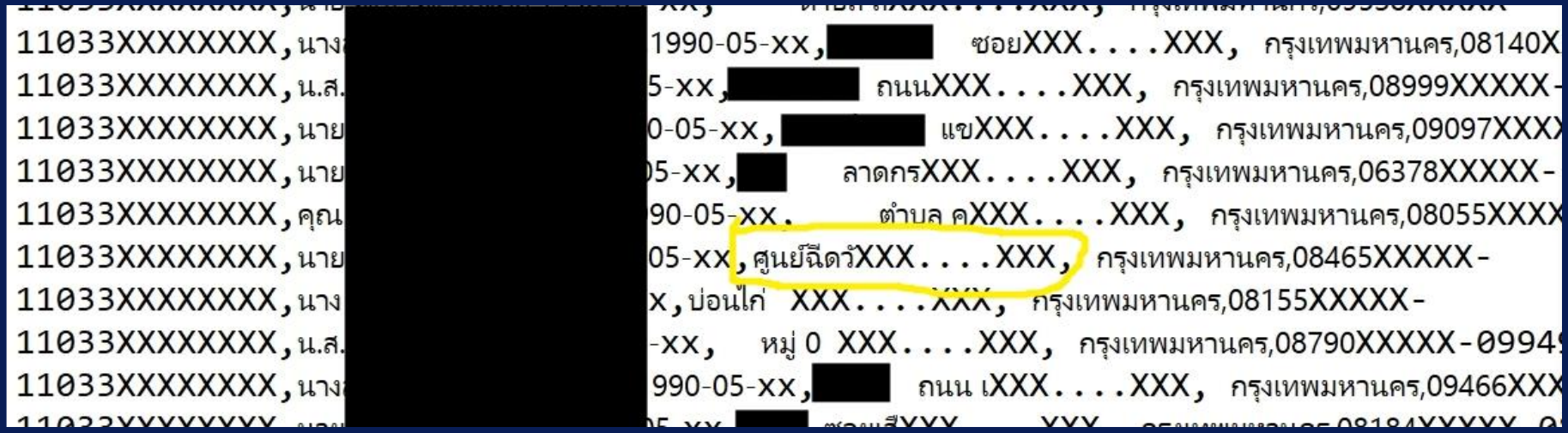
https://breached.vc/ (Now Taken Down)

Preliminary Data Assessment

- คำนำหน้าชื่อ นอกจาก “นาย” “นาง” “นางสาว” แล้ว ยังมีฐานันดรและยศ เช่น “หม่อมหลวง” “ว่าที่พ.ต.ต.” และ “ร้อยเอก” เป็นต้น ด้วย และมีคำนำหน้าชื่อที่ไม่เป็นทางการในระบบราชการด้วย เช่น “นายแพทย์” “แพทย์หญิง” “ทพ.ดร.” “นพ.”
- แต่จากการตรวจสอบเบื้องต้น ไม่พบคำนำหน้าชื่อที่เป็นยศทหารระดับนายพันหรือนายพล (อาจเป็นเพราะโดยอายุใน sample data ที่เกิดปี ค.ศ. 1990 ทำให้ยังมีอายุงานและประสบการณ์ไม่ถึงระดับชั้นยศนั้น)
- ทั้งนี้ การที่มีคำนำหน้าชื่อที่ไม่เป็นทางการ เช่น “นายแพทย์” ฯลฯ ด้วย แสดงว่าน่าจะเป็นฐานข้อมูลอื่นที่ไม่ใช่ทะเบียนราษฎร และการที่มีทั้ง “นายแพทย์” และ “นพ.” แสดงว่าน่าจะมีแหล่งที่มาของข้อมูลจากหลายแหล่งประกอบเข้าด้วยกัน

https://breached.vc/ (Now Taken Down)

Interesting Data



https://breached.vc/ (Now Taken Down)

https://breached.vc/ (Now Taken Down)

ผลการเปรียบเทียบข้อมูลใน sample data ที่ถูกละเมิดกับฐานข้อมูลผู้ป่วยของ รพ.รามาธิบดี

รายการ	จำนวนแถว (rows)	ร้อยละ (%)
Total rows	93,154	
หลังตัดชื่อที่ซ้ำกันออก (After data deduplication)	86,571	100%
ชื่อ-นามสกุล มีในฐานข้อมูลผู้ป่วยของ รพ.รามาธิบดี	15,057	17%
ชื่อ-นามสกุล มีในฐานข้อมูลผู้ป่วยของ รพ.รามาธิบดี และเกิดปี ค.ศ. 1990 จากฐานข้อมูลผู้ป่วยของ รพ.รามาธิบดีจริง	11,543	13%

https://breached.vc/ (Now Taken Down)

ผลการเปรียบเทียบข้อมูลใน sample data ที่ถูกละเมิด กับฐานข้อมูลผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี ตั้งต้นจากฐานข้อมูลผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี

รายการ	จำนวนราย	ร้อยละ (%)
ผู้ได้รับวัคซีน COVID-19 ที่ รพ.รามาธิบดี	415,418	
ผู้ได้รับวัคซีน COVID-19 ที่ รพ.รามาธิบดี และเกิดปี ค.ศ. 1990	9,711	100%
เลขประจำตัวประชาชน 5 ตัวแรก (ที่ไม่ถูกปกปิด) + ปีเกิด + นามสกุล มีในฐานข้อมูลผู้ได้รับวัคซีน COVID-19 ที่ รพ.รามาธิบดี	3,205	33%

หมายเหตุ : เหตุผลที่ต้องใช้เงื่อนไข เลขประจำตัวประชาชน 5 ตัวแรก (ที่ไม่ถูกปกปิด) + ปีเกิด + นามสกุล ในการเปรียบเทียบระหว่าง 2 ฐานข้อมูล เพราะมีข้อจำกัดในการใช้ชื่อ-นามสกุล เนื่องจากคำนำหน้าชื่อใน sample data มีหลายรูปแบบ ไม่สามารถ clean data ได้ทุก pattern (เช่น มีทั้งคำนำหน้าชื่อที่มีเว้นวรรคหน้าชื่อ และที่ไม่มีเว้นวรรคหน้าชื่อ และมีคำนำหน้าชื่อที่หลากหลาย ทั้งยศ คุณวุฒิทางวิชาชีพ (เช่น นายแพทย์ แพทย์หญิง) คุณวุฒิระดับปริญญาเอก (ดร.) อยู่ด้วยในหลาย pattern จึงไม่สามารถ clean data ในส่วนของชื่อให้สมบูรณ์เพื่อนำมาใช้เปรียบเทียบได้ จึงจำเป็นต้องใช้เฉพาะนามสกุลมาเปรียบเทียบร่วมกับเงื่อนไขอื่นแทน

แปลผลโดยการอนุมาน (1)

- ผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี จะมีโอกาสที่จะถูกละเมิดข้อมูลส่วนบุคคลในกรณีนี้มากพอสมควร (โดยยังไม่ยืนยันว่าแหล่งที่มาที่ทำให้ข้อมูลรั่วไหลคือแหล่งใด)
- อย่างไรก็ตาม ร้อยละที่ผู้มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี จะมีโอกาสที่จะถูกละเมิดข้อมูลส่วนบุคคลในกรณีนี้ ยังไม่สูงมากพอที่จะเป็นข้อมูลส่วนใหญ่ของ sample data กล่าวคือ ผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี ยังไม่ใช่ majority ของ sample data ที่ถูกละเมิด
- เหตุการละเมิดข้อมูลส่วนบุคคลนี้จึงน่าจะเกิดขึ้นในระดับประชากร (population) ที่ใหญ่กว่าผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี แต่มีความเป็นไปได้ที่ผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดีจะเป็นส่วนหนึ่งของข้อมูลที่ถูกละเมิดด้วย

https://breached.vc/ (Now Taken Down)

ผลการเปรียบเทียบข้อมูลใน sample data ที่ถูกละเมิด กับฐานข้อมูลผู้ที่มารับวัคซีน COVID-19 ที่ รพ.รามาธิบดี ตั้งต้นจากข้อมูลใน sample data ที่ถูกละเมิด

รายการ	จำนวนราย	ร้อยละ (%)
Total rows	93,154	
หลังตัดชื่อที่ซ้ำกันออก (After data deduplication)	86,571	100%
เลขประจำตัวประชาชน 5 ตัวแรก (ที่ไม่ถูกปกปิด) + ปีเกิด + นามสกุล มีในฐานข้อมูลผู้ได้รับวัคซีน COVID-19 ที่ รพ.รามาธิบดี	3,205	4%

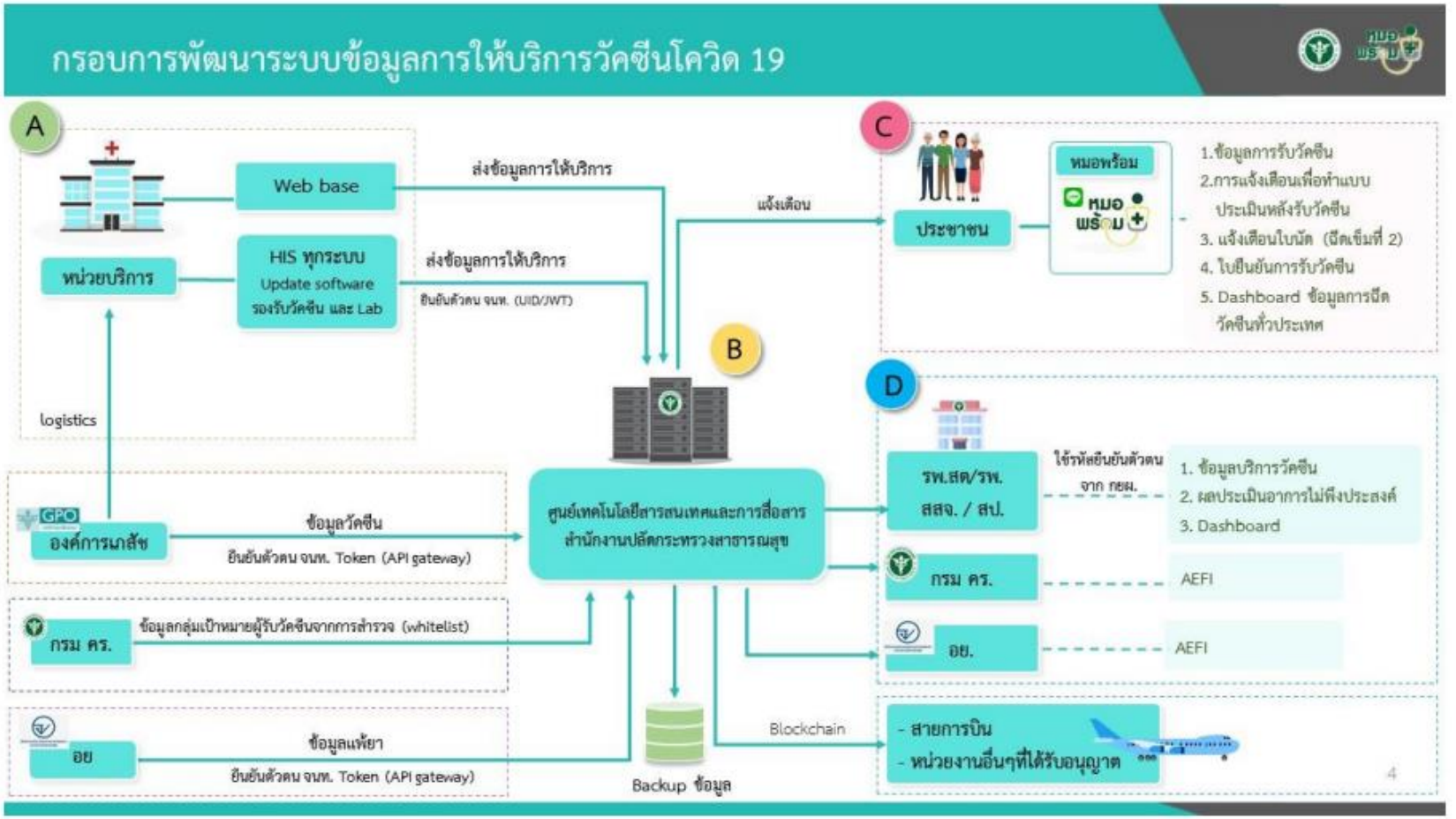
หมายเหตุ : เหตุผลที่ต้องใช้เงื่อนไข เลขประจำตัวประชาชน 5 ตัวแรก (ที่ไม่ถูกปกปิด) + ปีเกิด + นามสกุล ในการเปรียบเทียบระหว่าง 2 ฐานข้อมูล เพราะมีข้อจำกัดในการใช้ชื่อ-นามสกุล เนื่องจากคำนำหน้าชื่อใน sample data มีหลายรูปแบบ ไม่สามารถ clean data ได้ทุก pattern (เช่น มีทั้งคำนำหน้าชื่อที่มีเว้นวรรคหน้าชื่อ และที่ไม่มีเว้นวรรคหน้าชื่อ และมีคำนำหน้าชื่อที่หลากหลาย ทั้งยศ คุณวุฒิทางวิชาชีพ (เช่น นายแพทย์ แพทย์หญิง) คุณวุฒิระดับปริญญาเอก (ดร.) อยู่ด้วยในหลาย pattern จึงไม่สามารถ clean data ในส่วนของชื่อให้สมบูรณ์เพื่อนำมาใช้เปรียบเทียบได้ จึงจำเป็นต้องใช้เฉพาะนามสกุลมาเปรียบเทียบร่วมกับเงื่อนไขอื่นแทน

แปลผลโดยการอนุมาน (2)

- ผู้ที่มีรายชื่อใน sample data ที่ถูกละเมิด จะมีโอกาสเป็นผู้ที่มารับวัคซีน COVID-19 ที่โรงพยาบาลรามาธิบดี**น้อยมาก** (ประมาณ 4% หากพิจารณาจากผู้ที่เกิดปี ค.ศ. 1990)
- โดย**ผู้ที่มีรายชื่อใน sample data ที่ถูกละเมิด ส่วนที่เหลืออีกเป็นสัดส่วนจำนวนมาก น่าจะไปรับวัคซีน COVID-19 ที่โรงพยาบาลอื่นที่ไม่ใช่** รพ.รามาธิบดี

https://breached.vc/ (Now Taken Down)

ระบบ MOPH Immunization Center



ภาพที่ 1 ภาพแสดงกรอบการพัฒนาระบบข้อมูลการให้บริการวัคซีนโควิด 19 กระทรวงสาธารณสุข

https://mohpromt.moph.go.th/mpc/wp-content/uploads/2021/10/manual_vaccine-V11.pdf

ประเด็นที่ควรพิจารณา

ในทาง Cybersecurity และในทางคดี

1. มี (หรือน่าจะมี) การกระทำความผิดเกิดขึ้นหรือไม่
2. หากมี ผู้ใดเป็นผู้กระทำความผิด มีพยานหลักฐานเพียงใด
3. หากมี ถือเป็นเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือไม่ และเกี่ยวข้องกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หรือไม่
4. หากเป็น และเกี่ยวข้อง หน่วยงานดังกล่าวมีหน้าที่ตามกฎหมายอย่างไร

https://breached.vc/ (Now Taken Down)

ประเด็นที่ควรพิจารณา

ในทางการคุ้มครองข้อมูลส่วนบุคคลและ PDPA

1. มี (หรือน่าจะมี) เหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ และจะพิจารณาอย่างไร

2. หากมี ผู้ใดมีหน้าที่ตามกฎหมาย PDPA และมีหน้าที่อย่างไรบ้าง

https://breached.vc/ (Now Taken Down)

Personal Data Breach Notification

หน้า ๗
เล่ม ๑๓๙ ตอนพิเศษ ๒๙๒ ง ราชกิจจานุเบกษา ๑๕ ธันวาคม ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

"การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

ข้อ ๔ เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยเหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่น โดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๒) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

(๓) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

ข้อ ๕ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าโดยทางวาจา เป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเอง ว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

(๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่ โดยผู้ควบคุมข้อมูลส่วนบุคคลพึงดำเนินการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังกล่าว ทั้งในส่วนที่เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณารายละเอียดจากข้อเท็จจริงที่เกี่ยวข้อง รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

(๒) หากระหว่างการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลตาม (๑) พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติม โดยทันทีเท่าที่จะสามารถกระทำได้ ทั้งนี้ อาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยีที่จำเป็นและเหมาะสม

(๓) เมื่อพิจารณาจากข้อเท็จจริงตาม (๑) แล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

(๔) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

(๕) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

ข้อ ๗ ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานโดยเร็ว ทั้งนี้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

https://ratchakitcha.soc.go.th/documents/17233460.pdf

Personal Data Breach Notification

ข้อ ๑๒ ในการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด ผู้ควบคุมข้อมูลส่วนบุคคลอาจพิจารณาจากปัจจัยดังต่อไปนี้

(๑) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

(๒) ลักษณะหรือประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๓) ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด ซึ่งอาจพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลหรือจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๔) ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ รวมถึงข้อเท็จจริงว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ ประกอบด้วยผู้เยาว์ ผู้พิการ ผู้ไร้ความสามารถ ผู้เสมือนไร้ความสามารถ หรือบุคคลเปราะบาง (vulnerable persons) ที่ขาดความสามารถในการปกป้องสิทธิและประโยชน์ของตนเนื่องจากข้อจำกัดต่าง ๆ ด้วยหรือไม่ เพียงใด

(๕) ความร้ายแรงของผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการละเมิดข้อมูลส่วนบุคคล และประสิทธิผลของมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหายต่อการบรรเทาผลกระทบและความเสียหายที่เกิดขึ้นหรืออาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

(๖) ผลกระทบในวงกว้างต่อธุรกิจหรือการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลหรือต่อสาธารณะจากเหตุการละเมิดข้อมูลส่วนบุคคล

(๗) ลักษณะของระบบการจัดเก็บข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด และมาตรการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งที่เป็นมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) รวมถึงมาตรการทางกายภาพ (physical measures)

(๘) สถานะทางกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลว่าเป็นบุคคลธรรมดาหรือนิติบุคคล รวมทั้งขนาดและลักษณะของกิจการของผู้ควบคุมข้อมูลส่วนบุคคล

https://ratchakitcha.soc.go.th/documents/17233460.pdf

ประเด็นที่ควรพิจารณา (เพิ่มเติม)

ในทางการคุ้มครองข้อมูลส่วนบุคคลและ PDPA

1. มี (หรือน่าจะมี) เหตุการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่ และจะพิจารณาอย่างไร

2. หากมี ผู้ใดมีหน้าที่ตามกฎหมาย PDPA และมีหน้าที่อย่างไรบ้าง

3. กรณีที่มีหน่วยงานที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบหรือ data source เดียวกันหลายหน่วยงาน ควรดำเนินการอย่างไร

4. กรณีที่ไม่ปรากฏพยานหลักฐานที่ชัดเจน หรือไม่มี log ที่ตรวจสอบได้ ควรทำอย่างไร และเมื่อใดจะถือว่า “มีเหตุอันควรเชื่อได้ว่ามีเหตุการละเมิดข้อมูลส่วนบุคคล” (“a reasonable degree of certainty” that a breach has occurred. [EDPB Guidelines 9/2022 on personal data breach notification under GDPR Version 2.0, Adopted 28 March 2023])

5. หากน่าจะเกิดเหตุก่อน PDPA บังคับใช้ จะต้องแจ้งเหตุหรือไม่

6. ความรับผิดทางกฎหมายในกรณีที่มีเหตุการละเมิดข้อมูลส่วนบุคคลเป็นอย่างไร

https://breached.vc/ (Now Taken Down)

Lessons Learned

- การพัฒนาระบบที่ประมวลผลข้อมูลส่วนบุคคล ควรคำนึงถึงความเสี่ยงด้าน cybersecurity & personal data breaches เป็นพิเศษโดยเฉพาะหากมี sensitive personal data เช่น ข้อมูลสุขภาพ
- การเร่งพัฒนาระบบในสถานการณ์ฉุกเฉิน ควรคำนึงถึงความเสี่ยงด้าน cybersecurity & personal data breaches ให้ได้สัดส่วนกับความจำเป็นเร่งด่วน (โดยเฉพาะกรณีเป็น large-scale processing) และควรเร่งปิด gap โดยเร็วเท่าที่จะทำได้
- หลักความรับผิดชอบ (Accountability) ของผู้ควบคุมข้อมูลส่วนบุคคล
- ไม่ว่าจะมองว่า (วงการ)หมอพร้อมหรือไม่พร้อม เราก็ต้องพัฒนา cybersecurity & privacy safeguards ของงานด้าน digital health ต่อไป และเรียนรู้และปรับปรุงจากทุกเหตุการณ์ที่เกิดขึ้น

https://breached.vc/ (Now Taken Down)