Deloitte.

Conversations with Deloitte Thailand

Conversations with Deloitte Thailand - Podcast
January 2021
EP. 7 - Data Leakage
Dr. Wit Sitthivekin
Parichart Jiravachara, Partner, Risk Advisory Services Deloitte Thailand

Synopsis
In a data driven world, data is being used and transferred everywhere around us. Organisations use data for their businesses, to stay competitive and to stay relevant. Personal data or some types of data in organisations is considered as confidential. We all know the benefits of data but are we aware of the importance of protecting data and the risk of data leakage? How do we protect our data? What actions we should take when our data is leaked?

Dr. Wit | The previous episode, we talked about data and the risk of data leakage from Khun Parichart. I have to say well done, very good information indeed.

Parichart | Before we discuss further, next time please be careful about showing your thumb.

Dr. Wit | Why not? Giving thumbs up is an expression for approval. Everyone knows that.

Parichart | Your fingerprints might be captured.

Dr. Wit | Even from this angle? Is it that easy?

Parichart | With today's technology, it is possible.

Dr. Wit | Normally, Thai people believe that even if the data is leaked, it is not of a use of anybody. Anything you can share with us on how the leaked data has negative affects to personal or organization?

Parichart | We never know how organizations handle our data or how well they protect our data. We can assume that the organization a good data protection system but who knows. How can we be sure that our data is handle properly?

Dr. Wit | So the basic information that we usually give away is name / surname/ and mobile phone number, is it risky to provide this information?

Parichart | Actually, this kind of data is classified as sensitive information according to the Personal Data Protection Act. Name, surname, address, mobile number can identify a person.

Dr. Wit | So, this is sensitive information?

Parichart | Yes, and we give this information by ourselves.

Parichart | Yes, we are the one who allow them to use our data but how we can confident that during the process, our data is well protected. Who keep it? How is it used? How is it destroyed after the program is done? We know nothing.

Dr. Wit | What are security measures for protecting sensitive and confidential information nowadays?

Parichart | For Financial Sector, they have measurements for data security for quite some time now but other sectors are only starting. Because they only start to have incidents about data leakage.

Dr. Wit | Financial sector, I got it because it concerns money and stuff but other sector, what are their concern?

Parichart | For example a factory, we thought that there is nothing. But there are production recipes and processes that are important?

Dr. Wit | Trade secrets.

Parichart | Yes, actually there are sensitive information for every industry but the problem is businesses do not know that this or that information is their sensitive information. They do not know which data is Sensitive, Confidential, Internal Use or Publicly Available, hence they cannot classify their data.

Dr. Wit | So how do we help our clients who would like to do data security. Can you share with us, step by step?

Parichart | Deloitte has what it is called Data Protection Framework. This Data Protection Framework is a guideline on what organizations need to do. We can start with Data Protection Assessment. Because data leakage can happen in many ways. Not just through the system. Sometimes through a paper that we accidentally place somewhere that contains sensitive information.

Dr. Wit | A paper document is still risk?

Parichart | Yes, therefore we can help our

their Potential Data Leakage Maturity to find out areas that need improvement. Then, we give them recommendations. Sometimes raising awareness among the employee is enough. Employees may not have practical knowledge about Data Leakage and Personal Data Protection Act. Some other cases, it may be the processes that need improvement, whether manual or automate.

Dr. Wit | Automate means system so could you explain how we protect data leakage using systems?

Parichart | There is the technology called Data Classification Tool that can help us. For examole when we save a file, a system will ask whether this file is Sensitive / Confidential or Internal Use. If it contains Confidential Information but we want to save as Internal Use, the tool will not allow as this file contains Confidential Information. So you can only save the file as Confidential Information only.

Dr. Wit | What are confidential information?

Parichart | Business Strategy, Network Diagram, Production process/ formula. Actually, classifications depend on each organization.

Dr. Wit | So, how can the system identify which is sensitive information which is confidential?

Parichart | The tool is very smart. We set the rules and put in keywords for the system.

Dr. Wit | Yes, but sometimes it depends on human as well, especially, authorized persons. Sometimes it is the authorized persons that do unauthorized things.

Parichart | | Yes, nowadays we have the technology called Database Monitoring which is the system that monitoring DBA or how's authorized person do with data and what type of data they can access.

Dr. Wit | To monitor authorized persons.

Parichart | Yes.

Dr. Wit | What about USB. We save our work on USB. How do we protect it?

Parichart | For Deloitte, the hard disk of all employees has password. In case the hard disk or notebook is lost, other people cannot access data. We also have the Procedure that employee needs to report office and tell the police. Also, we didn't allow employees to save document in Thump Drive. This is Minimum Requirement to protect our data. We give similar recommendation s to clients. For the financial sector, as Data Leakage is very important, they even make USB port unavailable for use.

Dr. Wit | Employees cannot transfer data to external device, right?

Parichart | Definitely yes, cannot save any data to external device.

Dr. Wit | So that employees need to stick with the devices or anything that can access data by using password only.

Parichart | Correct. If any employee needs to have data and would like to send the data to their personal e-mail account, if the organization that very serious about this, they will have Data Leakage Tool which monitoring the mai gateway. Also, the tool will know that who sending sensitive information to personal email or not. But nowadays we need to bring work to work at home, in this case the organization need to weight whether they will allow Sensitive I nformation to be stored in employee's notebook or not. Or how do they monitor their employees' notebooks. Everything requires People Process and Technology.

Dr. Wit | Just print it out then, make it easy.

Parichart | Actually, printed document is the most difficult to control

Dr. Wit | So, how do we protect data on printed material?

Parichart | There is the technology called Digital Rights Management. I can send a file to a recipient and set up open time within 7 days, if that person didn't open the file within 7 days, the file will no longer be accessible. I can also set that this file cannot be printed out.

Dr. Wit | So how should organization start?

Parichart | Do the assessment first, classify the data we have, then identify the potential leak channels.

Dr. Wit | We may have outsourcing staff.

Parichart | Yes. Housekeeper, etc. There are many channels that data can leak. Network system should be evaluated first to identify the required steps and actions. We may already have standard policy and procedures but may not yet roll out or implement it.

Dr. Wit | We already have it somewhere.

Parichart | But have not yet bring it to practice.

Dr. Wit | So we need to be careful with everything. Digital world has its disadvantages.

Parichart | Exactly, you need to sacrifice some conveniences for security.

Dr. Wit | Indeed! Thank you Khun Parichart.

Deloitte.

Conversations with Deloitte Thailand

Conversations with Deloitte Thailand - Podcast

มกราคม 2021

ตอนที่ 7 - เมื่อข้อมูลสำคัญหลุดบนโลกไซเบอร์

ดร. วิทย์ สิทธิเวคิน

ปาริชาติ จิรวัชรา พาร์ทเนอร์ บริการด้านความเสี่ยงองค์กร ดีลอยท์ ประเทศไทย

Synopsis

ข้อมูลส่วนบุคคล หรือข้อมูลบางประเภทขององค์กร ถือว่าเป็นข้อมูลที่สำคัญและควรถูกเก็บไว้ให้ปลอดภัย จากผู้ไม่หวังดีที่ประสงค์จะมาขโมยข้อมูลของเราไป เพื่อหาผลประโยชน์ อย่างไรก็ตาม ในปัจจุบันหลายๆ คนและองค์กรยังไม่ได้ตระหนักถึงความสำคัญของ การเก็บรักษาข้อมูลของตนเอง และความเสี่ยงที่เกิด ขึ้นจากการรั่วไหลของข้อมูล เราจะป้องกันไม่ให้ข้อมูล สำคัญรั่วไหลออกไปได้อย่างไร และควรทำอย่างไร เมื่อข้อมูลสำคัญหลุดออกไป?

ดร. วิทย์ | | FYI by Deloitte ตอนที่แล้วนะครับ เรา พูดถึงเรื่องข้อมูลปัจจุบันครับ บอกว่า ข้อมูลของเรา มีคน Hack ออกไปได้ความรู้มากมายเลยจากคุณ ปาริชาต หรือ พี่ตุ๋ม ต้องบอกว่า เยี่ยมมาก งวดที่แล้ว

ปาริชาติ | ก่อนจะไปถึงตรงนั้นนะคะ คราวหลังอย่า เยี่ยมมากแล้วชูนิ้วโป้งออกนะคะ

ดร. วิทย์ | | อ้าวทำไมละพี่ เป็นท่าที่มาตรฐานมาก สมัยนี้ เวลาจะทำอะไรก็ทำแบบนี้

ปาริชาติ | มีคนอาจจะ Capture ลายนิ้วมือเราไป แล้วก็ได้นะคะ

ดร. วิทย์ | มันง่ายขนาดนั้นเลยเหรอพี่ ขนาดมุมไกลๆ แบบนี้นะฮะ

ปาริชาติ | ด้วยเทคโนโลยีของกล้องปัจจุบันเนี่ย คม ชัดเจนมาก

ดร. วิทย์ | | ที่นี้ผมต้องถามพี่ โดยปกติคนไทยเราเชื่อ แบบนี้ เรื่อง Data Leakage หรือว่าข้อมูลที่รั่วไหลไป เขาเอาไปทำอะไรไม่ได้หรอก จริงๆ แต่ขนาดเดียวกันก็ จะมีคนที่ล้วงข้อมูลออกไป เอาข้อมูลออกไปขยายผล มีประเด็นอะไร หรือว่ามีเรื่องราวอะไรหลักๆ บางไหม ครับที่บอกว่า การเอาข้อมูลปลอมออกไปใช้ แล้วมัน สร้างผลเสียต่อบุคคลหรือองค์กรครับ

ปาริชาติ | คือในบางครั้ง บางกรณี เราไม่รู้เลยจริงๆ ว่าข้อมูลที่เราให้กับองค์กรในฐานะที่เราเป็นผู้ใช้บริการ แล้วองค์กรดูแลปกป้องข้อมูลของเราอย่างไร บาง ครั้ง องค์กรอาจจะมีวิธีการปกป้องที่ดีอยู่แล้ว แต่ ในบางกรณี เราไม่รู้ว่าผู้ดูแลระบบ ที่มีสิทธิ์สูงสุดใน ระบบ เขาอาจจะทำอะไรที่เกินเลยขอบเขตหน้าที่งาน เขาหรือเปล่า เราจะมีการ วิธีการ Detect หรือจับได้ อย่างไรว่า ผู้ดูแลระบบที่สามารถเข้าถึงข้อมูลได้ จะไม่ เอาข้อมูลของเราออกไปขายให้ข้างนอก ซึ่งอาจจะส่ง ความเสียหายให้กับทั้งองค์กรเอง แล้วก็ผู้ใช้บริการ อย่างพวกเรา

ดร. วิทย์ | โอ้ ถ้าพูดแบบนี้เราขยับตัวยากเหมือนกัน นะครับ ปัญหาที่หลายๆ คนคิด พี่ตุ๋มลองยกตัวอย่าง ได้ไหม ข้อมูลสมมตินะครับ ผมไปสมัครชิงโชคอะไรสัก อย่าง แค่ ชื่อคนนี้ นามสกุลนี้ เบอร์โทรศัพท์นี้ มันก็ไม่ เป็นเป็นไรหรือเปล่าครับพี่

ปาริชาติ | จริงๆ พวกนั้น ถูก Classifieds ว่าเป็น Sensitive Information ตาม พ.ร.บ.คุ้มครองข้อมูล ส่วนบุคคลเลยนะคะ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ สามารถ Identified ได้ว่าบุคคลนั้นคือใคร

ดร. วิทย์ | นี่เขาถือว่า Sensitive ละ

ปาริชาติ | ใช่ เราเป็นคนกรอก

ดร. วิทย์ | ครับ ด้วยตัวเราเอง

ปาริชาติ | ด้วยตัวเราเองด้วย เราอนุญาตให้เขา เอาไปทำ แต่ในระหว่างทางเรามั่นใจได้ไงตอนที่เรา หย่อนชุดคูปองชิงโชคเนี่ย กล่องที่รับเก็บ ใครเป็นคน ดูแล ใครเป็นคนปกป้อง มีการเก็บรวบรวมอย่างไร แล้วหลังจากที่มีการชิงรางวัลจับรางวัลแล้ว มีการ ทำลายเอกสารเหล่านั้นอย่างไร

ดร. วิทย์ | ผมถามในแง่ของมาตรการในการดูแล ความปลอดภัยไม่ให้ข้อมูลเหล่านี้ Sensitive ก็ดี Confidential ก็ดี รั่วไหลออกไป มันมีความรัดกุม ขนาดไหนแล้วครับ ปัจจุบัน

ปาริชาติ | จริงๆ หลายๆ องค์กรเนี่ย ถ้าไม่นับที่เป็น Financial Sector ก็พึ่งเริ่ม หรือมาเริ่มเพราะมี Incident เกิดขึ้น มี Data Leakage ก็เลยอยากที่จะ ดูแลปรับปรุง ถ้าเป็น Financial Sector เขาเริ่มทำ มาระยะหนึ่งแล้ว

ดร. วิทย์ | | อ้าว งั้นผมถาม Financial Sector เรา เข้าใจเป็นเรื่องการเงินการทอง แล้ว Sector อื่นที่เขา ก็ไม่น่ามีอะไร มันก็ไม่ใช่เรื่องเงินเรื่องทอง มีเรื่องอะไร ที่มันดูน่ากลัวหรือพี่

ปาริชาติ | อย่างโรงงาน เราคิดว่าก็ไม่น่ามีอะไรถูก ไหมคะ สูตรการผลิต สำคัญไหมคะ

ดร. วิทย์ | อ่อ ความลับทางการค้าเลยนะ

ปาริชาติ | ใช่ จริงๆ ในทุกๆ Industry จะมี Sensitive Information แต่ปัญหาคือว่า Business รู้หรือเปล่า ว่าข้อมูลเหล่านั้นเป็น Sensitive Information ของ องค์กร เพราะจุดเริ่มต้นเลยอันดับแรก ลูกค้ามักจะ ไม่รู้ว่า จริงๆ แล้วเขามี Data ที่เป็น Sensitive หรือ

Confidential หรือ Internal Use หรือ Publicly Available เพราะเขาไม่รู้ว่าเขามี Data อะไรบ้าง เขาก็ไม่รู้ว่าจะจัดลำดับความสำคัญอย่างไร

ดร. วิทย์ | ทาง Deloitte เนี่ยให้คำแนะนำคนที่ต้องการจะดูแลความปลอดภัยของข้อมูลของตัวเองให้คำแนะนำสมมุติเป็นขั้นเป็นตอน พาเราเดินไปหน่อยได้ไหมครับทำอย่างไรบ้าง

ปาริชาติ | คือจริงๆ แล้ว Deloitte เนี่ยเราจะมีตัว Data Protection Framework อยู่นะคะ ตัว Data Protection Framework เนี่ยจะช่วย Guide ลูกค้าว่าในแง่ของ Governance Structure ในแง่ของ Policy Process Procedure ในแง่ของ System เนี่ย ในแต่ละ Layer เนี่ย เรามีวิธีการดูแลปกป้องยังไง ลูกค้ามักจะบอก อ๋อ ไม่รู้หรอก ถ้างั้นเราทำ Data Protection Assessment ใหม่ เพราะว่าการที่ Data จะรั่วไหลออกจากองค์กรได้เนี่ย มีมากมายหลายวิธี มันไม่ใช่แค่รั่วทางระบบ มันอาจจะเป็นกระดาษที่บังเอิญเราไปวางทิ้งไว้ที่ไหนแล้วมันเป็น Sensitive Information

ดร. วิทย์ | ใช้กระดาษยังเสี่ยงอีกหรือพี่

ปาริชาติ | ใช่ค่ะ คือมันมีแนวทางในการ Leak ได้หลากหลาย โดยจุดเริ่มต้นเราจะช่วยลูกค้าในการประเมินก่อนว่า โอเค Potential Data Leakage Maturity ของคุณเป็นอย่างไง มี Area ไหนบ้างที่ต้องได้รับการ Improve แล้วเราก็จะให้ Recommendations เพราะว่าในบางเรื่อง มันอาจจะปิดได้แค่เรื่อง Awareness ก็ได้ พนักงานอาจจะไม่ได้มีความตระหนักรู้เกี่ยวกับเรื่อง Data Leakage อาจจะไม่ได้ตระหนักรู้เรื่องเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เรื่องอะไรที่เกี่ยวข้องกับตัวคุ้มครองข้อมูลส่วนบุคคล รวมถึง Cyber หรืออาจจะปิดด้วย Process เช่น อย่างที่เรียนคะว่า องค์กรจะต้องมี Information Classification Policy Standard and Procedure มีทำอะไร ถ้าเราเจอคำว่า Sensitive บนเอกสาร พนักงานต้องรู้ว่าโอเค ถ้าเป็น Sensitive ไม่ควรวางบนโต๊ะ ควรจะเก็บใส่ลิ้นชักล็อก ถ้าจะส่งต่อให้คนอื่นต้องใส่ซองที่ Seal เข้ารหัส ถ้าจะส่ง File นี้ที่เป็น Sensitive ควรจะมีการ Encrypt ก่อนที่จะส่งให้คนอื่น เพราะฉะนั้นปกติเนี่ยเราก็จะดู 2 เรื่องนี้เป็นหลักก่อน เสร็จแล้วเราก็จะดูว่าเทคโนโลยีอะไรที่สามารถช่วยให้ลูกค้า Automate Process เหล่านี้ได้

ดร. วิทย์ | Automate มีความหมายว่าไม่ได้พึ่งตัวคนละ พึ่งตัวระบบ ในฐานะที่ผมไม่ใช่คนที่รู้เรื่องเทคโนโลยีนะครับ ผมอยากให้พี่อธิบายในเรื่องของ Data Leakage ผ่านตัวระบบก่อน แล้วเราใช้เทคโนโลยีอะไรเข้ามาช่วยป้องกัน ก่อนที่จะไปถึงตัวบุคคลนะฮะ เอาที่ตัวระบบก่อนนะพี่

ปาริชาติ | ปัจจุบันมีเทคโนโลยีเขาเรียกว่า Data Classification Tool เวลาเราเปิด File ขึ้นมา เราทำงาน พอเราจะกด Save มันก็จะถามว่า โอเค File นี้นะ จะเป็น Sensitive หรือเป็น Confidential หรือเป็น Internal Use ให้ User หลอก ทั้งๆ ที่มันมี Confidential Information แต่เราอยากจะ Save เป็น Internal Use Tool มันจะบอกว่าไม่ได้ ในเมื่อ File นี้มี Confidential Information นะ คุณต้อง Save เป็น Confidential Information เท่านั้น

ดร. วิทย์ | ขออนุญาต เบรก ถามเลย Confidential ที่พี่พูดถึงได้แก่อะไรบ้างครับ คือ Sensitive เราพอเข้าใจละว่าอาจจะมีความอ่อนไหว ถึงระดับที่บอกว่าเป็น Confidential มันมีอะไรบ้างครับพี่

ปาริชาติ | ค่ะ อย่างถ้า Confidential โดยปกติก็คือจะเป็นพวก Business Strategy เราคงไม่ได้อยากเปิดเผย Network Diagram ถ้าเกิดคนอื่นรู้ หรือแม้กระทั่งข้อมูลที่เกี่ยวข้องกับสูตรการผลิตบางที่เขา Classify ว่าเป็น Confidential จริงๆ Classification เนี่ยขึ้นอยู่กับองค์กรเลยค่ะ ถ้าเป็นหน่วยงานราชการเนี่ยเขาก็จะมี พ.ร.บ. การจัดลำดับชั้นข้อมูลข่าวสาร มันก็จะมี 5 ชั้น บางองค์กรก็จะมี 4 ชั้น อันนี้แล้วแต่ไม่ได้มี Fix ตายตัวว่าจะมีกี่ Class

ดร. วิทย์ | ครับ เป็นแบบนี้ ที่นี้พอบอกว่ามันมีกลไกที่สามารถที่จะ Labelling ได้ สมมุติ User ไปหลอกละไม่ใช่ Confidential ไม่ใช่ความลับ แต่เป็น Sensitive มันรู้ได้ไงครับ

ปาริชาติ | Tool มันฉลาดคะ เพราะว่าเราใส่ Keyword เข้าไป ให้มัน Detect ว่าคำไหนคือ Contain Confidential Information ฉะนั้นส่วนหนึ่งเนี่ยเทคโนโลยีต้องใช้ร่วมกับผสมผสานกับที่ปรึกษาค่ะออกแบบว่าจะ Set Rule ยังไงให้มัน Detect เจอได้

ดร. วิทย์ | | ครับ แต่บางครั้งระบบทั้งหมดก็คงไม่ใช่ที่สุดมันก็ขึ้นอยู่กับตัวบุคคล โดยเฉพาะอย่างยิ่งคนที่ถือกุญแจ IT องค์กร ที่จะสามารถทำสิ่งต่างๆ ได้อย่างที่พี่ตุ้มบอกนะ สิ่งที่น่ากลัวคือ Authorised People คนที่มีอำนาจ คนถือกุญแจเนี่ย Do Unauthorised things ไปทำสิ่งที่ไม่ถูกต้อง

ปาริชาติ | ค่ะ ด้วยปัจจุบันเนี่ยมันมีเทคโนโลยีที่เขาใช้เรียกว่า Database Monitoring คะ คือคอย Monitor ดูว่า DBA ผู้ดูแลระบบฐานข้อมูลเนี่ยทำอะไรเกี่ยวกับ Data บ้าง เข้าถึงข้อมูลไหนบ้างนะคะ

ดร. วิทย์ | คือไป Monitor คนถือกุญแจอีกชั้นนึง อันนี้ดูด้วยระบบ

ปาริชาติ | ดูด้วยระบบ อันนี้ต้องพึ่งพิงระบบอย่างเดียวเลยค่ะ หรือแม้กระทั่งบางครั้งผู้ดูแลระบบเองลาพักร้อน ต้องมีการ Delegate ให้กับน้องๆ ในทีม เขาเองก็กังวล เวลาเขากลับมาว่า น้องเราไปทำอะไรหรือเปล่า ในบางเทคโนโลยีนะคะ สามารถย้อนเรียกกลับดูได้เป็น VDO เลยนะคะว่าเขาเข้าไปทำอะไรบ้าง เปลี่ยนแปลงข้อมูลอะไรไปบ้าง

ดร. วิทย์ | แต่อย่างเวลาที่โลกนี้ปัจจุบันเวลาเราใช้ต้องบอกว่ามันไม่ได้ Stick อยู่กับตัว Device ติงต่าง คนทำงาน Save ใส่ USB USB หาย ข้อมูล Leak ไปที่อื่น จะดูแลกันยังไงครับ

ปาริชาติ | คือจริงๆ อย่างของดีลอยท์เอง Hard Disk ของพนักงานของเราทุกคนเนี่ย ก็คือมีการเข้ารหัส ในกรณีที่ Hard Disk หาย เออ Notebook หายก็ไม่สามารถเข้าถึงเนื้อ Data ได้ เราก็จะมี Procedure ว่าเขาต้อง Report ทาง Office นะคะ แล้วก็จะมีการแจ้งความ ในขณะเดียวกันถ้าเกิดจะเอาข้อมูลที่อยู่ใน Notebook เนี่ย Save ใส่ Thump Drive Thump Drive นั้นต้องเข้ารหัส ถ้าไม่งั้น Office จะไม่อนุญาตให้คุณ Save งานออกใส่ Thump Drive ได้ นี่ก็จะเป็น Minimum Requirement ที่เราดูแล ปกป้อง เราก็จะให้ Recommendation ให้กับลูกค้าคล้ายๆ กัน เดี๋ยวนี้เนี่ยในสถาบันการเงินแล้วก็องค์กรที่ค่อนข้าง Serious เกี่ยวกับ Data Leakage เขาจะปิด USB Port เพราะ USB Port

ดร. วิทย์ | ไม่สามารถเอา External ไปจุ๊บออกมาได้ถูกไหม

ปาริชาติ | ใช่ อันนั้นคือ Definitely ห้าม Save อะไรออกเลย

ดร. วิทย์ | เพราะงั้นก็ต้อง Stick อยู่กับ Device หรืออะไรก็ตามที่สามารถ Access ได้ด้วย Password เท่านั้น

ปาริชาติ | ใช่ค่ะ หรือถ้าเกิดพนักงานจะต้องการเอาข้อมูลออก บางคนเนี่ย ส่งไปที่ Personal E-mail Account ถ้าองค์กรนั้น Serious มากๆ เขาจะมี Tool Data Leakage คอย Monitor ที่ Mail Gateway เลยคะ ว่าคุณส่ง Sensitive Information ไปที่ Personal E-mail หรือเปล่า บางคนพนักงานบางที่ บอกว่าก็ต้องเอางานกลับไปทำที่บ้านนี่ ทำอย่างไง ฉะนั้นองค์กรก็ต้อง Weight ว่าคุณจะยอมให้ Sensitive Information ของคุณไปเก็บอยู่ที่ Notebook ของพนักงานที่บ้านหรือเปล่า คุณจะ Weight เรื่องนี้ยังไง คุณจะคอย Monitor เรื่องนี้ยังไง ทุกอย่างมันก็พึ่งพาด้วย People Process และ Technology

ดร. วิทย์ | ทำไปทำมาบางคนบอกกลัวจังเลยโลก Digital งั้นก็ส่งง่ายๆ เลย Print ออกมา

ปาริชาติ | จริงๆ การ Print เป็นอันที่ Control ยากที่สุด

ดร. วิทย์ | แล้วเรามีวิธีการดูแลไหมครับ อ้าวบางทีเราส่งข้อมูล Sensitive Confidential ไป ก็ Print อะ ก็น่าจะปลอดภัยไหมครับพี่

ปาริชาติ | คือ ถ้าเรากลัวขนาดนั้นเนี่ย มันก็จะมีอีกเทคโนโลยีนึงก็คือ Digital Rights Management ส่ง File ที่เป็น Sensitive ไป ตุ้มให้เวลา 7 วัน ถ้าไม่เปิดอ่าน Access ไม่ได้ แล้วตุ้มบังคับด้วยว่าห้าม Print

ดร. วิทย์ | นี่มันบังคับขนาดนั้นเลยเหรอฮะ ห้าม Print ได้อีก คุยกันมาถึงตรงนี้หลายๆ องค์กรที่อาจจะมีข้อมูลที่เยอะมากมาย อาจจะเริ่มต้นไม่ถูก จะ Classify ยังไง สมมุติว่าให้พี่ตุ้มมีคำแนะนำ ว่าถ้าเกิดว่าจำเป็นต้องทำ พิจารณาทีละขั้นทีละขั้น ดีลอยท์จะให้คำแนะนำอะไรเป็นพิเศษบ้างครับ

ปาริชาติ | คือในเรื่องดูแลปกป้องข้อมูลนี่ค่ะ อันดับแรกถ้าถามความคิดเห็นตุ้ม ตุ้มคิดว่าเราควรทำ

Assessment ก่อนดูสิว่าเรามีข้อมูลอะไรบ้างที่สำคัญ มาตรการในการดูแลปกป้องของเรามีอะไรบ้าง ปัจจุบันมันมี Channel ไหนบ้างที่ Data มี Potential ที่จะ Leak ออกไป อย่างที่เราคุยกันมา Third party ก็มีโอกาส ในบางครั้ง Office ของเรา มีผู้บริการคนอื่นเข้ามาเดินเพ่นพ่านใน Office ของเราไหม

ดร. วิทย์ | เช่น Outsource เข้ามา Maintain อะไรก็แล้วแต่

ปาริชาติ | ใช่ แม่บ้าน อย่างนี้เป็นต้น ถูกไหมคะ Channel มีตั้งเยอะไม่ได้หลุดเฉพาะระบบ Network เราควรจะเริ่มทำการประเมินก่อน พอประเมินแล้วเนี่ย เราก็จะได้รู้ว่า Step หรือ Action ที่เราควรจะเดินต่อคืออะไร เพราะบางที่อาจจะมีพวก Policy Standard Procedure อยู่แล้ว แต่ถามว่าเรื่อง Role Out ละ การนำไปปฏิบัติใช้มีเปล่า ยัง มีแค่ Policy เหมือนอยู่ใน

ดร. วิทย์ | คือมี Concept อยู่ในกระดาษอะไรอย่างนี้นะ

ปาริชาติ | แต่ไม่ได้มีการนำมา Practice

ดร. วิทย์ | รัดกุมเกินไปทุกอย่างมันก็อึดอัด รัดกุมด้วยแต่ในขณะเดียวกันก็มีความยืดหยุ่นพอให้ได้สะดวกสบายมันมี Solution ไหมครับว่าจะทำยังไงให้รู้สึกว่าเราไม่ต้องระวังจนวิตกกังวลและเดินหน้าในการใช้ชีวิตในโลก Digital ได้ลำบาก

ปาริชาติ | คือจริงๆ Security ต้องแลกกับความสะดวกสบายระดับนึง

ดร. วิทย์ | อาจจะสะดวกสบายน้อยลงนะครับ แต่ท้ายที่สุดก็ได้ความปลอดภัยกลับมาด้วยนะครับ โลก Digital ยุคนี้สะดวกสบายขึ้นก็จริงนะครับ แต่เรื่องของการที่ข้อมูลจะ Leak ออกไปและถูกนำไปใช้ในทางที่ไม่ถูกต้องก็มี ดังนั้นการวางระบบเอาไว้ การจัดลำดับชั้นข้อมูลก็น่าจะเป็นสิ่งที่ปลอดภัยมากขึ้น และนี่ก็คือ FYI by Deloitte ครับ