Deloitte.

Conversations with Deloitte Thailand

Conversations with Deloitte Thailand - Podcast
January 2021
EP. 6 - Cyber Risks
Dr. Wit Sitthivekin
Parichart Jiravachara, Partner, Risk Advisory Services Deloitte Thailand

Synopsis
These days, It is easy to access information in the cyber world. However, some people do not realize that their information, especially for the company, can be violated or taken advantages of. What are those risks people should be aware of and how to secure confidential information?

Parichart | Some of us like to take our mobile phone with us to the restroom. How can we be sure that the phone is safe and not hacked? You may appear in a video that spreading all over the internet.

Dr. Wit | Today, we will talk about an issue that is really close to us. We can freely surf the internet or cyber world but it also means that someone might be able to access to our personal data. Despite security and measures, how can we be sure that we are safe are we in the cyber world? Today, we are with Khun Parichart Jirawatara to talk about Cyber Risk. First of all, we all have devices such as tablet and smartphone. Are we at risk? Is information in our devices well protected.

Parichart | Let's start with a simple stuff. If we jailbreak our smartphone, how can we be sure our smart phone camera was not hacked.

Dr. Wit | It is simple like that?

Parichart | Yes, it is. We always bring a smartphone to the restroom. If your phone is hacked and camera was activated, you may live from the restroom without knowing it. However, nowadays there is a sticker or mobile phone camera cover to protect the camera from being accessed.

Dr. Wit | If an individual like us is at risk, would it be higher risk or organisations? Or we can build defense wall? They say that Cyber risk is evolving every day, is that true?

Parichart | That is true. People think technology can solve everything but it is actually us, the people that are the no.1 risk factor. How much do we know about data protection? Let's say, Facebook, do we know how to set up Privacy? Do we know that our posts should be set up as "Personal" only, not Public? Or do we know what we should or should not post or share? We don't know what Facebook do with our data. Therefore, before Post, Share or whatever, we need to think first.

Dr. Wit | Because in the Cyber world, it is not a one on one communication.

Parichart | Also, younger generations always take photos, post and share, even at a meeting. After the meeting is finished, they feel like celebrating that the project is completed and they take a selfie then and there, with a business strategy plan as a background. Then, they post it on social media without realising it.

Dr. Wit | So confidential information was leaked to the public by themselves.

Parichart | Exactly. At Deloitte, we have a service called "Cyber Watch". We monitor if there is any photos that contains sensitive information and notify the clients if we found them. There are many leakage cases of selfie photos after a meeting with sensitive information in the photos.

Dr. Wit | Who would have thought, right? That is why we need an expert because they know where the risks are. Now, as an organisation, I believe they would have some level of cyber security in place. But the bad guys would always try their best to access our information. How do we know whether the security system in our organisation is enough?

Parichart | Currently, organisational Cyber Security Assessment has become a trend. It is an annual assessment of organisation's data protection capabilities, similar to our annual physical check up. We have a physical check up every year to identify any health issues we may have in order to receive a proper treatment or prevent new health issues. The same concept apply to Cyber Security Maturity Assessment – to identify organisation's risk issues and seek preventive solutions, whether it concerns People, Process or Technology. In some organisations, it may be a lack of staff's awareness. So the Cyber Security Maturity Assessment will help organisations to identify areas of improvement.

Dr. Wit | I think one topic concerning cyber risk that is scary to us is data leakage. I believe that Deloitte has an extensive experience on this as well. How do we prevent data leakage?

Parichart | We do. A framework is a good start. One topic under this framework is Information Asset. Normally, every organisations have assets such as tables, chairs, notebooks, etc. Everyone says data is important. Network accessories, computer and server is important but we do not have this things listed.

Dr. Wit | I remember when I was young, our school desk had these stickers.

Parichart | And we never classify that which data is sensitive or confidential either.

Parichart | When the data is classified, we know which data is sensitive, which is confidential. Then we bring in technology and process.

Dr. Wit | Many people use technology first. But actually it is the organisation's requirements and risk assessment first, then the solution.

Parichart | Exactly. It is like we are protecting our home. Why we keep money and valuable items in a safe box. It is because we classified that those things are valuable. So that is why it is kept in the safe box in our bedroom, with double lock door. Some might also have CCTV installed. The same idea apply to our organisation. There are a lot of important data but we have never classified which data is important. Another difficulty that we faced with our clients is they do not know where the data is or which data is important. They need us to analyse and classify it for them.

Dr. Wit | What data can be identified as important data?

Parichart | Organisation strategy. A production formula, for example.

Dr. Wit | A trade secret.

Parichart | Organisation Network Diagram, Source Codes, etc. Hackers are looking to snatch this information.

Dr. Wit | Is there many hackers today, some might ask? And do they always look for an opportunity to hack us all the time?

Parichart | We have heard about Cloud as a service, Software as a service, Application as a Service. These days, there is Hacking as a service.

Dr. Wit | Very interesting word. What does it mean?

Parichart | There is a hacker service. And it is available on the internet.

Dr. Wit | Like hiring a gunman?

Parichart | You can buy the service and pay by bitcoin.

Dr. Wit | They are in the dark, we are in the open. Now, how do we do the risk assessment, or identify threats - what is the process?

Parichart | Actually, most leading organisations have a Security Operating Center or SOC to monitor cyber threats. Deloitte also have SOC around the world working 24/7 monitoring any potential threats for clients.

Dr. Wit | Technology is important for sure but I think another thing that is also important is people. They can strengthen or weaken the organisation. How do we prepare people in the organisation?

Parichart | Many organisations start to realise that people actually are important factor for the organisations' cyber security. Some organisations run Cyber Security Awareness Program. It has to be a program running through out, not a project.

Dr. Wit | Long term.

Parichart | Yes. For example, during new staff orientation program, organisation should share their company cyber security policy as well.

Dr. Wit | To make them realise how important it is.

Parichart | Yes. And a company should have e-learing or class room trainings on Cyber Security for their staff. Some organisation have it in a game format to test the level of understanding of their staff. Some holds a Security Day - setting up booth to educate the safe ways to do Facebook security setting or how to set a safe and secure CCTV at home. Because CCTV can also be hacked. Or even a simple thing that was mentioned earlier that younger generations like to post everything on social media. Good days or bad days, they take photos. They spill coffee on a table, they take photos without realising that there is sensitive information in the photos that they share on Facebook.

Dr. Wit | So the company's confidential information is leaked unintentionally. So how about print it on the paper, put it in a box and seal the box. It should be more secure this way?

Parichart | There is another issue called "Third Party Risk". There was an incident with printed documents in a country in this region last year. The said document was to be taken to the storage. The document was left unguarded in front of the office building in central business district, waiting for the document storage company to pick them up. By the time the document storage company come to pick them up, some of the document was blown away by the wind. Later, we found out that the document contain sensitive information. So there was a regulatory penalty for that. The organisation was fined for the incident. Even though our organisation have a good security and good protection, but the damage might happen because of a third party such as our business partner.

Dr. Wit | Third Party Risk means risks from third party. The case we discussed earlier happened to printed data. What about the third party in the digital world. How do we ensure the safety and security of the system?

Parichart | A simple example is Cloud. We can compare Cloud to living in a condominium. How can we be totally confident about safety & security living in a condominium? Each room in the condominium has its own protection on a different level. If the room owner do not have a good security or if the condominium do not have a good security system, someone might break into the room or the condominium. For example, IT person may not know how to install the system securely and incidentally spreading confidential information to public. It is like you open the door and welcome a bad person into your house.

Dr. Wit | Thank you so much. We have learned a lot today that we need to be aware of the cyber risks and learn how to protect ourselves and our organisation.

Deloitte.

Conversations with Deloitte Thailand

Conversations with Deloitte Thailand - Podcast

มกราคม 2021

ตอนที่ 6 - ความเสี่ยงบนโลกไซเบอร์

ดร. วิทย์ สิทธิเวคิน

ปาริชาติ จิรวัชรา พาร์ทเนอร์ บริการด้านความเสี่ยงองค์กร ดีลอยท์ ประเทศไทย

Synopsis

ทุกวันนี้ข้อมูลต่างๆสามารถเข้าถึงได้อย่างสะดวกรวดเร็วผ่านทางโลกไซเบอร์ แต่คนหลายๆคนยังไม่เคยตระหนักรู้ว่าข้อมูลที่อยู่บนโลกไซเบอร์ของตนเองหรือบริษัทมีความเสี่ยงต่อการถูกละเมิด และนำไปใช้ในทางที่ไม่ถูกต้องได้หลายช่องทาง ความเสี่ยงเหล่านั้นมีอะไรบ้าง? และเราหรือบริษัทควรทำอย่างไร?

ปาริชาติ | พวกเราชอบถือมือถือเข้าห้องน้ำ แล้วมั่นใจได้ยังไงว่า กล้องนั้นไม่ถูก Hacker คุณอาจจะมีหนังสดเปิดเผยในที่สาธารณะ

ดร. วิทย์ | FYI by Deloitte ในวันนี้นะครับ เป็นเรื่องประเด็นใกล้ตัวมากๆ เลย เราอาจจะสามารถเข้าไปท่องโลก Internet หรือโลก Cyber ได้เป็นอย่างดี แต่ขณะเดียวกันก็มีความหมายว่า คนอื่นก็สามารถเข้าถึงข้อมูลของเราได้เช่นเดียวกัน ถึงแม้จะมีเรื่องของ Security และมาตรการต่างๆ แล้วก็ตามนะครับ ใครจะไปรู้ครับว่า เราจะมีความปลอดภัยขนาดไหน วันนี้ครับ เราจะได้พูดคุยกับคุณปาริชาติ จิรวัชรา นะครับ ซึ่งเป็นผู้ที่จะมาพูดคุยกับเรา เกี่ยวข้องกับเรื่องของ-Cyber Risk แรกทีเดียวผมเรียนถามพี่ตุ๋มก่อน พูดถึงความเสี่ยง เอาพวกเราก่อน พวกเรามี Device ใช่ไหมครับ เรามี Tablet เรามีโทรศัพท์มือถือ Smart Phone เรามีความเสี่ยงไหมครับ เพราะเขาบอกว่า ปัจจุบันข้อมูลต่างๆ ถูกปกป้องเอาไว้เป็นอย่างดี

ปาริชาติ | เอาเรื่องง่ายๆ เลย กล้องบนมือถือ ถ้ามือถือเรา Jailbreak เรามั่นใจได้ยังไงว่า กล้องนั้นไม่ถูก Hack

ดร. วิทย์ | มันมาง่ายอย่างนั้นเลยหรือครับ

ปาริชาติ | ใช่ พวกเราชอบถือมือถือเข้าห้องน้ำ ถ้ากล้องนั้นถูก Activate โดย Hacker คุณอาจจะมีหนังสด เปิดเผยในที่สาธารณะได้ ปัจจุบันนี้เขามีอุปกรณ์หรืออาจจะมี Sticker ที่แปะเพื่อป้องกันกล้อง ไม่ให้มีคนสามารถ Access ได้

ดร. วิทย์ | ถ้าภาคประชาชนยังมีความเสี่ยงรอบตัวขนาดนี้ ลองคิดดูแล้วกันครับว่า Data ขององค์กรต่างๆ น่าจะมีความเสี่ยงมากกว่าไหมครับ หรือ เราสามารถที่จะ Build กำแพงต่างๆ ป้องกันได้ ผมถามกับพี่ในเรื่องของ Risk ในโลก Cyber ปัจจุบันมันเขาบอกว่ามันมีวิวัฒนาการทุกวัน จริงไหมครับ

ปาริชาติ | จริงค่ะ แต่ว่าในบางกรณี เรื่องความเสี่ยงบางคนคิดว่าใช้เทคโนโลยีปิดได้ทุกอย่าง จริงๆ ความเสี่ยงที่น่ากลัวที่สุดคือมาจากคน ตัวเรานี่เอง เรามีความตระหนักมากน้อยแค่ไหน ในการ Protect และดูแลข้อมูล ยกตัวอย่างง่ายๆ Facebook เรารู้ไหมคะว่าเราเคยตั้ง Privacy ไหม รู้ว่าสิ่งที่เรา Post มันควรเป็น Personal เท่านั้นไม่ใช่ Pubic หรือของบางอย่างจำเป็นต้อง Post ไหม จำเป็นต้อง Share ไหม เราไม่รู้เลยว่า Facebook เอาข้อมูลเราไปทำอะไร ฉะนั้นก่อน Post ก่อน Share อะไรก็แล้วแต่ คิดหนึ่งครั้งก่อน

ดร. วิทย์ | เพราะโลก Cyber ไม่เหมือนเดิม ไม่ใช่สื่อสารแบบหนึ่งต่อหนึ่งอีกต่อไปแล้ว

ปาริชาติ | แล้วเด็ก Gen ใหม่ สมัยนี้ชอบถ่ายรูป ชอบ Share เวลาไปเข้า Meeting พอ Meeting เสร็จแล้ว Strategy เสร็จแล้ว ผลงานเสร็จแล้ว Selfie กันหน่อย Selfie แต่ข้างหลังยังมี Strategy Plan แล้วคุณก็ Post ขึ้น Facebook

ดร. วิทย์ | ข้อมูลก็เลย Leak ออกสู่ภายนอกจากตัวเราเอง

ปาริชาติ | ใช่ จริงๆ อย่างดีลอยท์ ก็มีบริการ Cyber Watch ให้ลูกค้า คือคอย Monitor ดูว่า มีภาพอะไรที่ Contain Sensitive Information ไหม หลุดแล้วก็แจ้งลูกค้า เราเจอ Case แบบนี้เยอะค่ะ Selfie เวลาประชุมจบ Sensitive Information ทิ้งนั้นเลย

ดร. วิทย์ | ใครไปคิดนะครับ อันนี้ต้องใช้ Expert เลยนะ เขาจะได้รู้ว่าความเสี่ยงมาจากไหน ผมขอถามว่าแต่ละองค์กรก็คงจะมีความเชื่อมั่นในระบบของตัวเองนะครับว่า เรามีระบบ Security ความปลอดภัยในการที่จะลดความเสี่ยง Cyber ให้ได้เยอะที่สุด แต่ฝ่ายที่เขาอยากจะได้ข้อมูลเรา ก็คงจะมีพัฒนาการไปเรื่อยๆ ที่นี่เราจะรู้ได้ยังไงครับว่า ระบบที่เรามีอยู่ปลอดภัยเพียงพอหรือเปล่าครับ

ปาริชาติ | จริงๆ ปัจจุบันนี้จะมี Trend ในการทำ Cyber Security Assessment เป็นการประเมินประจำปี ว่าองค์กรเนี่ย มี Capability ยังไง ในการที่จะดูแลปกป้องข้อมูล หรือ System ของระบบภายในองค์กรยกตัวอย่างง่ายๆ เหมือนเรา ทุกปีเราไปตรวจสุขภาพ ถูกไหมคะ เราก็อยากรู้ Indication ต่างๆ เป็นเบาหวานไหม ค่าน้ำตาลเยอะไหม ไขมันในเส้นเลือดสูงไหม เพื่อที่เราจะได้ไปหาหมอเฉพาะทาง เฉพาะโรค ได้รับการรักษาที่ถูกต้อง ใน Concept เดียวกัน การประเมิน Cyber Security Maturity Assessment เพื่อให้เรารู้ว่า ความเสี่ยงขององค์กร มีด้านไหนบ้าง เพื่อหาวิธีการแนวทางแก้ไขได้ถูกต้อง เพราะว่าแนวทางแก้ไข มีทั้ง People Process Technology มันอาจจะเป็นด้านใดด้านหนึ่ง อย่างเรื่อง Awareness ของบุคลากร บางที่ไม่เคยทำ Awareness Staff ไม่เคยรู้ว่าเขาต้องทำอะไรบ้าง ฉะนั้นเราจะช่วยลูกค้าดูว่าหลังจากที่ประเมินแล้ว Area ไหนที่ควรได้รับการดูแลหรือ Improve ปรับปรุงพัฒนาให้มันดีขึ้น

ดร. วิทย์ | ผมว่าเรื่องของความเสี่ยงที่หลายคนกลัวมากๆ คือ เรื่องของการ Leak หรือการรั่วไหลของข้อมูล ดีลอยท์เองผมเชื่อน่าจะมีประสบการณ์ค่อนข้างเยอะ มาตรการในการที่เราช่วยลูกค้าให้สามารถที่จะป้องกันการรั่วไหลของข้อมูล เป็นยังไงบ้างครับ

ปาริชาติ | จริงๆ Framework นี้จะเป็นส่วนหนึ่ง จุดเริ่มต้นเลย ที่ลูกค้าควรที่จะนำมาใช้แล้วก็ประเมิน เพราะใน Framework จะมีการพูดถึง Information Asset Information Asset คืออะไร คือ ปกติในองค์กรพวกเราจะมีทะเบียนทรัพย์สิน โต๊ะ เก้าอี้ โน้ตบุ๊ก แต่ในเมื่อทุกคนบอกว่า Data สำคัญ ข้อมูลสำคัญ อุปกรณ์ Network สำคัญ Computer สำคัญ Server สำคัญ ทำไมเราไม่มีทะเบียนพวกนั้น

ดร. วิทย์ | ผมจำได้สมัยเด็กๆ เราจะมีแปะสติกเกอร์ไว้นะ โต๊ะอันนี้ อันนี้ ของหน่วยงานไหนนะ

ปาริชาติ | แล้วเราก็ไม่เคย จัดลำดับความสำคัญ ว่า Data ชุดนี้ คือ Sensitive คือ Confidential

ดร. วิทย์ | ไม่ได้ Classify ไม่ได้จัดลำดับเขาไว้

ปาริชาติ | พอเรา Classify เรารู้ว่ามัน Sensitive เรารู้ว่า Confidential เราค่อยหา Technology หา Process มาปิด เพราะเราคง Protect ทุกอย่างไม่ได้

ดร. วิทย์ | ผมเข้าใจแล้ว หลายๆ คนเอา Technology นำ อันนี้ไม่ใช่ เอาความจำเป็นขององค์กร การประเมินความเสี่ยงเป็นตัวนำไว้ก่อน จากนั้นเราก็มาหาวิธีการ

ปาริชาติ | ป้องกัน เหมือนเราที่บ้าน ทำไมแค่แก้วแหวนเงินทองเราถึงเอาเข้าตู้เซฟ เรา Classify แล้วว่ามันสำคัญ มันถึงได้รับการดูแลพิเศษ เข้าตู้เซฟ แล้วก็อยู่ในห้องนอนของเรา มีประตูล็อคอีกชั้น มีประตูบ้านอีกชั้น บางบ้านเครียดหนักมี CCTV อีก เหมือนกันค่ะ องค์กรของเรา มีข้อมูลที่สำคัญเยอะแยะ แต่เราไม่เคยจัดลำดับความสำคัญว่าข้อมูลนี้สำคัญหรือไม่สำคัญ ความยากที่เราเผชิญกับลูกค้าก็คือว่า ที่ปรึกษาเราไม่รู้หรอกนะว่า Data อยู่ที่ไหน ช่วยมาดูหน่อยสิว่า Data อยู่ที่ไหนบ้าง แล้วช่วยเขาในการวิเคราะห์ด้วย ข้อมูลนี้สำคัญหรือไม่สำคัญ

ดร. วิทย์ | ผมขออนุญาตถาม ข้อมูลสำคัญไม่สำคัญสมมุติลองเป็น Framework ทั่วๆ ไปนะครับ ข้อมูลที่สำคัญประกอบด้วยอะไรบ้าง

ปาริชาติ | อย่างง่ายๆ เลย คือ Strategy ขององค์กร สูตรการผลิต

ดร. วิทย์ | ซึ่งเป็นความลับทางการค้าอยู่แล้วนะครับ

ปาริชาติ | Network Diagram ขององค์กร ถ้าเกิดหลุดรั่วออกไปข้างนอก Hacker รู้ช่องทางดี Source Code ของโปรแกรม

ดร. วิทย์ | หลายคนถามมาเหมือนกันนะ Hacker ปัจจุบันมันเยอะขนาดนั้นเลยหรือครับ แล้วมันจ้องที่จะ Hack เราตลอดเวลาแบบนั้นเลยเปล่าครับ

ปาริชาติ | ใช่ค่ะ จริงๆ หลายคนพูดถึง Cloud as a service, Software as a service, Application as a Service ปัจจุบันนี้มี Hacking as a service

ดร. วิทย์ | มีความหมายว่าไรครับ คำนี้น่าสนใจมาก

ปาริชาติ | เราไม่จำเป็นต้องมี Hacker ภายในองค์กร คุณอยากใช้บริการ เข้าไป Internet

ดร. วิทย์ | เหมือนมือปืนรับจ้างอย่างงี้หรือครับ

ปาริชาติ | ซื้อบริการได้เลยค่ะ จ่ายเงินด้วย Bitcoin อยากจะยิงโจมตีคู่แข่งซื้อบริการได้เลยค่ะ ไม่แพง

ดร. วิทย์ | เขาอยู่ในที่มืด เราอยู่ในที่แจ้ง กระบวนการในการที่เราให้คำแนะนำลูกค้าก็ดี หรือกระบวนการที่เราจะ Assess ความเสี่ยง หรือไปดูว่า Threat หรือภัยคุกคามมาจากทางไหนเรามีวิธีการอย่างไรครับ

ปาริชาติ | จริงๆ ในองค์กรบริษัทชั้นนำใหญ่ๆ จะมีศูนย์เฝ้าระวังทางด้านภัยคุกคาม หรือเขาเรียก Security Operating Center ศูนย์ SOC นะคะ ศูนย์ SOC คอยเฝ้าระวังให้องค์กรต่างๆ ที่มาใช้บริการของเขา อย่างของดีลอยท์ ก็มีศูนย์ SOC ทั่วโลกเหมือนกัน ที่คอย Monitor ให้ลูกค้า 24 คูณ 7 แล้วก็มีให้รายงานออกไปว่า Potential ความเสี่ยง Threat ภัยคุกคามที่เกี่ยวข้องกับองค์กรของเขามีอะไรบ้าง เราอาจจะใช้บริการพวกนี้ได้

ดร. วิทย์ | เทคโนโลยีคงเป็นของตายนะครับ แต่ผมว่าสิ่งที่น่าจะสำคัญมากๆ คือเรื่องของการเตรียมบุคลากร เพราะบุคลากรจะทำให้องค์กรเข้มแข็งก็ได้จะทำให้องค์กรมีรูโหว่ก็ได้ ตรงนี้เรามีการช่วยกันเตรียมการ หรือหลักสูตรการฝึกอบรมพนักงานไหมครับว่าวิธีการในการที่จะระมัดระวังความเสี่ยงจากบุคลากรของแต่ละองค์กรจะเป็นไงบ้างครับ

ปาริชาติ | จริงๆ หลายๆ ที่ตอนนี้ Trends ของลูกค้าเริ่มตะหนักว่า คนเป็นจุดอ่อนที่สำคัญที่สุด ฉะนั้นเขาจะมีพวก Cyber Security Awareness Program เป็น Program นะคะ ไม่ได้เป็น Project เพราะมันต้อง Run through out

ดร. วิทย์ | ระยะยาวหน่อย

ปาริชาติ | ใช่ อย่างยกตัวอย่างง่ายๆ เวลาเรามีพนักงานเข้าใหม่ ในช่วงที่เรามี Orientation Program เราก็ควรที่จะมีการ Share เกี่ยวกับเรื่อง Security ขององค์กรด้วย

ดร. วิทย์ | ให้เขาเริ่มตะหนักว่ามิตินี้มันสำคัญขนาดไหน

ปาริชาติ | ใช่ ในระหว่างที่เขาทำงานกับองค์กรของเรา ก็อาจจะมีการให้ e-Learning หรือมี Classroom Training หรือบางที่เขาทำเป็นเล่นเกมส์ ดูว่าพนักงานมีความเข้าใจตัว Policy หรือเปล่า หรืออาจจะมีพวก Security Day ที่เห็นลูกค้าบางที่เขาทำ ก็คือ อาจจะมีการจัดบูธ ว่าจะ Set up Facebook ยังไงให้ปลอดภัย หรืออาจจะไปดูเรื่องกล้อง CCTV ที่บ้านเรา Hack ได้นะคุณควรจะได้ Set กล้อง CCTV ที่บ้านยังไงให้ปลอดภัย หรือแม้กระทั่งเรื่องง่ายๆ ใกล้ตัวอย่างที่เมื่อกี้เรียนก็คือว่า เด็ก Gen ใหม่สมัยนี้ Bad Day Good Day ก็ถ่ายรูป กาแฟหกใส่โต๊ะก็ถ่ายรูป แต่ที่โต๊ะมี Sensitive Information หรือเปล่าก็ไม่รู้ ถ่ายไป Post Facebook

ดร. วิทย์ | กลายเป็นเอาข้อมูลความลับของบริษัทออกไปหมดเลย คุยไปคุยมา บางคนบอก แบบนี้ดีไหม Print ใส่กระดาษ ใส่ลังเหมือนเดิม ซีลเอาไว้เลยเป็น Object ไม่มีใครสามารถโมยเราได้ ปลอดภัยกว่าไหมครับ

ปาริชาติ | จริงๆ มันก็จะมีอีก Issue หนึ่งนะคะ ซึ่งตอนนี้เป็น Trends เลยคือ Third Party Risk อย่างเมื่อต้นปีที่แล้ว มันมี Case อันหนึ่งที่ในประเทศในแถบภูมิภาคนี้ เขาเกิด Incident ก็คือเอกสารนี่แหละ เป็น Hard Copy เขาต้องการเอาไปเก็บที่คลัง เขาก็เอาลงไปไว้ที่หน้าตึกอยู่ในย่านธุรกิจ ปรากฏว่าไม่มีใครดูแลกว่าที่บริษัทเขาจะมาเก็บไปเข้าคลัง เอกสารนี่โดนลมพัดแล้วปลิว แล้วก็มีคนมาเจอว่าจริงๆ แล้วเป็น Sensitive Information ทั้งนั้น ไม่ว่าจะเป็นสถาบันการเงินหรือเป็นหน่วยงานอื่นๆ ก็โดนค่าปรับกันไปตามระเบียบ ต่อให้องค์กรของเรามี Protection ที่ดียังไงก็แล้วแต่ ถ้าคู่ค้าที่เราทำธุรกิจด้วย เขาไม่ได้ดูแลปกป้องอย่างดี มันอาจจะเป็นช่องทางหนึ่ง ที่ให้ Hacker สามารถเข้าถึงระบบเราได้

ดร. วิทย์ | | นี่ Third Party Risk มีความหมายคือความเสี่ยงจากบุคคลที่ 3 เมื่อสักครู่ เราพูดถึงตัวอย่างของ Hard Copy ใช่ ไหม ถ้าเป็นแบบ Digital World คนที่เป็น Third Party ทางเราเอื้อมมือเข้าไปดูแล ย้ำให้มั่นใจว่าเรามีความปลอดภัยทั้งระบบอย่างไรบ้างครับ

ปาริชาติ | | อย่างถ้า Case ใกล้ตัวที่เราเห็นในบ้านเราก็คือ Cloud หลายๆองค์กรใช้ Cloud เราไปใช้ Cloud เรามั่นใจได้ไง Cloud เหมือนคอนโดมิเนียม ถูกไหมคะ นิติบุคคลเป็นคนดูแล ห้องแต่ละห้องก็จะมีการดูแลปกป้องที่แตกต่างกัน ถ้านิติบุคล หรือเจ้าของห้องไม่รู้ว่าจริงๆ วิธีการดูแลปกป้องจะทำยังไง ที่ปลอดภัย ก็อาจจะมีความเสี่ยง อย่าง Case ที่เราเห็นในหน้าข่าว คนที่เป็นพนักงานทางด้าน IT ขององค์กรนั้นๆ อาจจะขาดความรู้ความเข้าใจในการติดตั้งค่าระบบยังไงให้มันปลอดภัยเลยทำให้ Incidentally มันเปิดเผยสู่สาธารณะคือ คนสามารถเข้าถึงได้ คือ คุณเปิดบ้านรอเขา มากกว่าที่จะปิดไม่ให้ใครเข้า

ดร. วิทย์ | คุยกับพี่ตุ่มได้ประโยชน์มากมายเลยนะครับ บางคนบอกว่าฟังแล้วกลัวไม่อยากใช้โลก Digital เลย แต่มันไม่ใช่นะครับ เพียงแต่เราต้องมีความระมัดระวังว่าโลก Cyber นี้ มีความเสี่ยงอะไรบ้าง เรามีความองค์ความรู้ว่าจะอุดรูรั่วมัน อย่างไร ไม่ว่าจะเป็นเรื่องของภาคบุคคลก็ดี หรือว่าขององค์กรก็ดี เราก็สามารถที่จะมีชัยในการที่จะดูแลข้อมูลของเราได้อย่างปลอดภัยไปด้วย และนี่แหละครับเป็นข้อมูลดีๆ จาก FYI by Deloitte ครับ