

Deloitte.



บทเรียนจากกรณีภัยไซเบอร์ที่เกิดขึ้นบ่อยครั้งในองค์กร
Case Studies related to Data Security and Protection
14 August 2018

Private and Confidential

Forensic 

Disclaimer

All materials or explanations (not restricted to the following presentation slides) (collectively "Material") have been and are prepared in general terms only. The Material is intended as a general guide and shall not be construed as any advice, opinion or recommendation.

In addition, the Material is limited by the time available and by the information made available to us. You should not consider the Material as being comprehensive as we may not become aware of all facts or information. Accordingly, we are not in a position to and will not make any representation as to the accuracy, completeness or sufficiency of the Material for your purposes.

The application of the content of the Material to specific situations will depend on the particular situations involved. Professional advice should be sought before the application of the Material to any particular circumstances and the Materials shall not in any event substitute for such professional advice.

You will rely on the contents of the Material at your own risk. While all reasonable care has been taken in the preparation of the Material, all duties and liabilities (including without limitation, those arising from negligence or otherwise) to all parties including you are specifically disclaimed.

บทเรียนจากกรณีภัยไซเบอร์ที่เกิดขึ้นบ่อยครั้งในองค์กร



About Deloitte Forensic

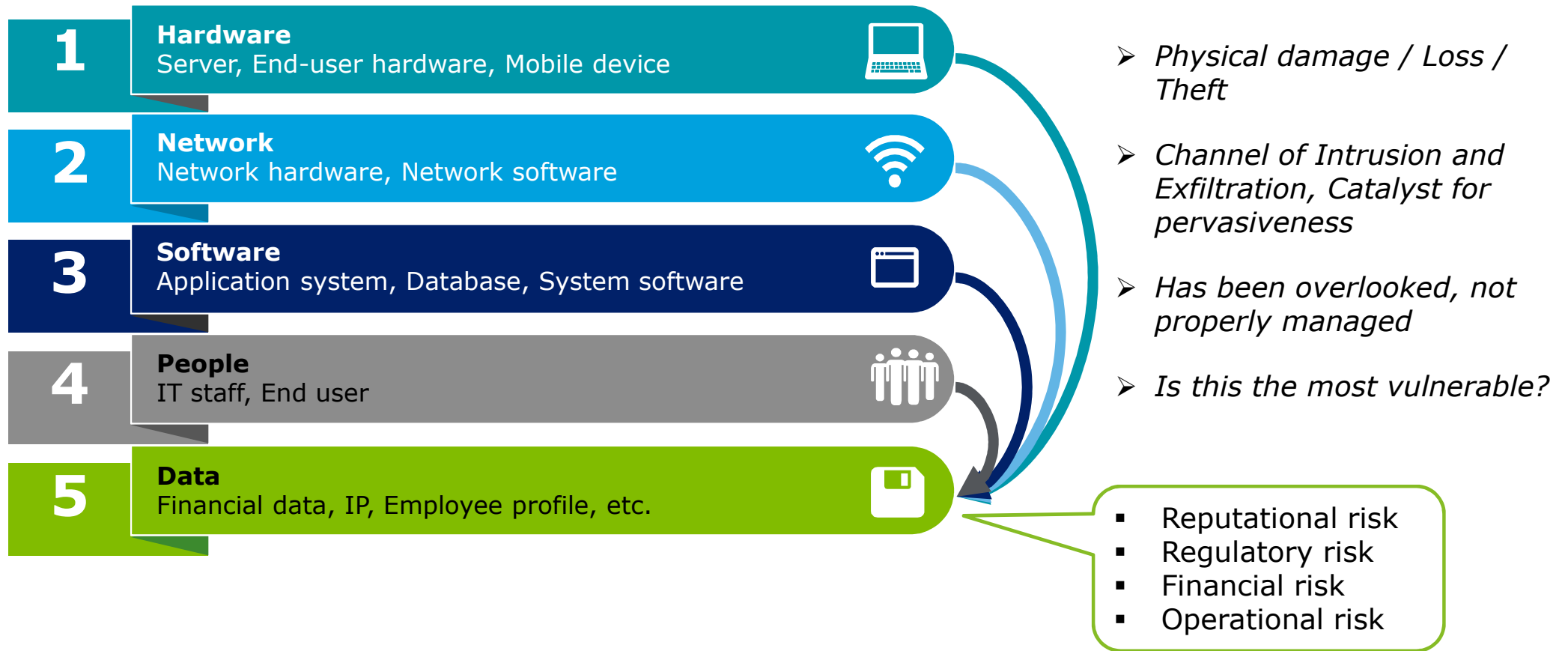
Why do we show up in a Cyber crisis?



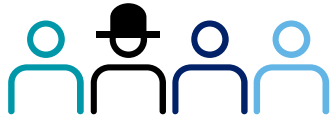
ภัยไซเบอร์ที่เกิดขึ้นบ่อยครั้งในองค์กร

แนวใหม่ และผลกระทบ

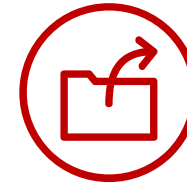
องค์ประกอบด้านเทคโนโลยีในองค์กร และภัยคุกคามในรูปแบบต่าง ๆ



แนวโน้มของภัยคุกคามทางไซเบอร์ The Changing Threat Landscape



- เกิดได้ทั้งจากบุคคลภายนอก และภายในองค์กร
- บุคคลภายในองค์กรที่กระทำการไปโดยไม่ได้มีเจตนา นั้น ถือเป็นปัญหาหลักขององค์กร
- การสร้างความรู้ความตระหนัก ผ่านการฝึกอบรม ตามบทบาทหน้าที่จะช่วยลดความเสี่ยงลงได้



- การเข้าถึงโดยมิชอบ และการเปิดเผยข้อมูลความลับขององค์กร หรือข้อมูลส่วนบุคคลถือเป็นแนวโน้มภัยคุกคามที่สำคัญ
- องค์กรต่าง ๆ ควรมีมาตรการในการเก็บรักษาข้อมูลสำคัญขององค์กร ที่เป็นไปตามมาตรฐานสากล และเป็นไปตามข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล
- มีการตรวจสอบมาตรฐานความปลอดภัยดังกล่าวอย่างสม่ำเสมอ

Source: IBM X-Force Threat Intelligence Index 2018

แนวโน้มของภัยคุกคามทางไซเบอร์ The Changing Threat Landscape



- ภัยคุกคามจากซอฟต์แวร์เรียกค่าไถ่ (Ransomware) และการทำลายข้อมูล (Data-wiping attacks) ยังคงมีเป็นหนึ่งในแนวโน้มที่สำคัญ
- ภัยคุกคามในรูปแบบดังกล่าว สร้างผลกระทบต่อการใช้งานสร้างความเสียหายทั้งในทางการเงิน และความน่าเชื่อถือขององค์กร



- แนวทางการป้องกันที่สำคัญยังคงเป็นเรื่องพื้นฐาน เช่น การติดตั้งตัวปรับปรุงหรือแก้ไขระบบ (Patch management) ทั้งในส่วนของ Hardware และ Software
- การนำเอาระบบการตรวจตรา (Monitoring system) แบบ Real-time รวมทั้งการใช้ปัญญาประดิษฐ์ (AI, Machine learning) มาใช้ในการตรวจจ็บบรูปแบบที่ต้องสงสัย จะช่วยในการตรวจจ็บบการบุกรุกได้อย่างทันที่ หรือทำนายการถูกโจมตีก่อนที่จะเกิดขึ้นได้

Source: IBM X-Force Threat Intelligence Index 2018

ความเสียหายจากภัยคุกคามทางไซเบอร์ Beneath the Surface of a Cyberattack

ค่าใช้จ่าย หรือ ความเสียหายที่เห็นได้ชัดเจน

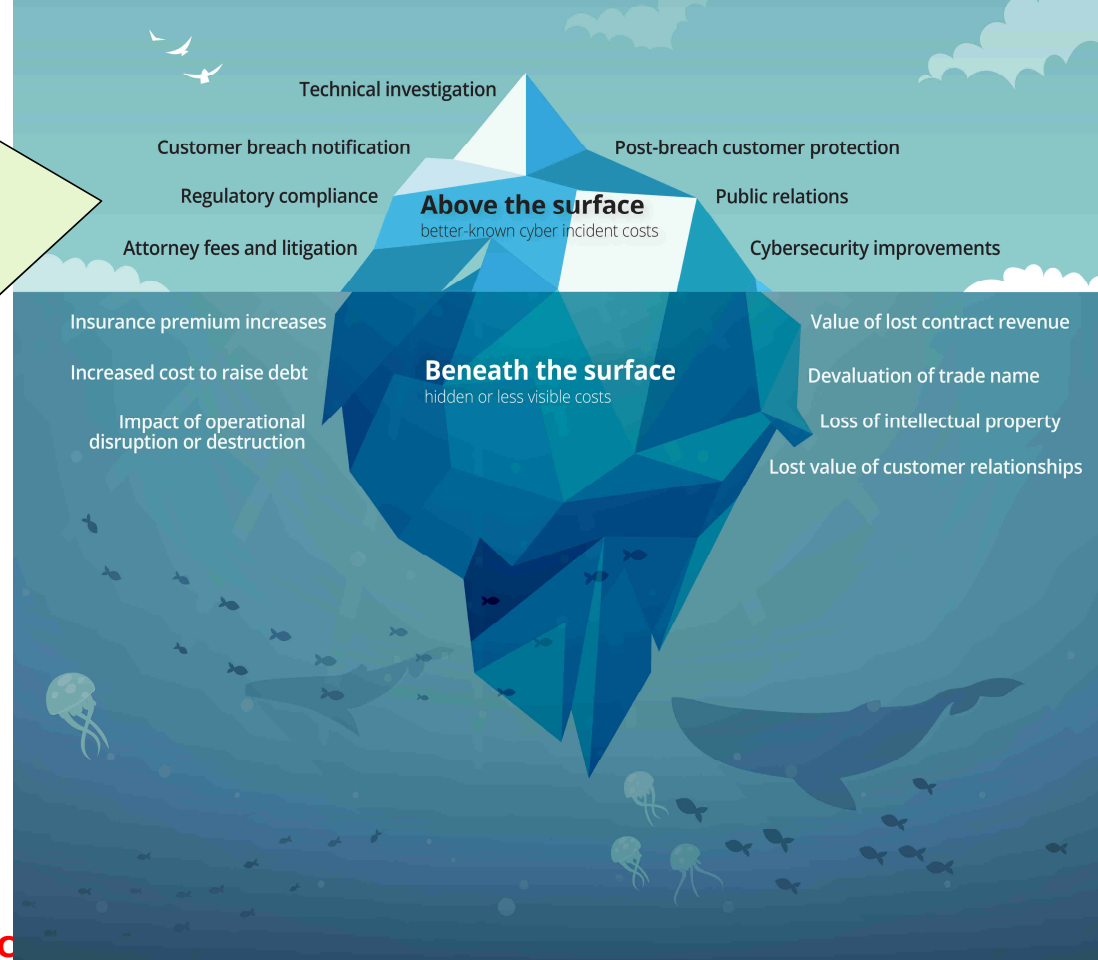
- การสืบสวนสอบสวน
- การแจ้งเตือนลูกค้าที่ได้รับผลกระทบ
- การป้องกันและรักษาผลประโยชน์ลูกค้าที่ได้รับผลกระทบ
- การปฏิบัติตามข้อกำหนดต่าง ๆ
- การสื่อสารกับสาธารณชน
- การดำเนินคดี หรือ การเกิดข้อพิพาทต่าง ๆ
- การปรับปรุงความมั่นคงปลอดภัยไซเบอร์

Source: Beneath the surface of a cyberattack, Deloitte

© 2018 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident



Private and C

ความเสียหายจากภัยคุกคามทางไซเบอร์ Beneath the Surface of a Cyberattack

ค่าใช้จ่าย หรือ ความเสียหายที่ซ่อนอยู่

- เบี้ยประกันภัยทางไซเบอร์ที่สูงขึ้น
- มูลค่าของสัญญาทางธุรกิจที่สูญหายไป
- ชื่อเสียงและความน่าเชื่อถือที่ลดลง
- ต้นทุนในการหาสินเชื่อใหม่ที่สูงขึ้น (อันเนื่องมาจากความน่าเชื่อถือที่ลดลง)
- ผลกระทบจากการปฏิบัติงานที่หยุดชะงักหรือถูกทำลาย
- การสูญเสียทรัพย์สินทางปัญญา
- การสูญเสียความสัมพันธ์กับลูกค้า

Source: Beneath the surface of a cyberattack, Deloitte

© 2018 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

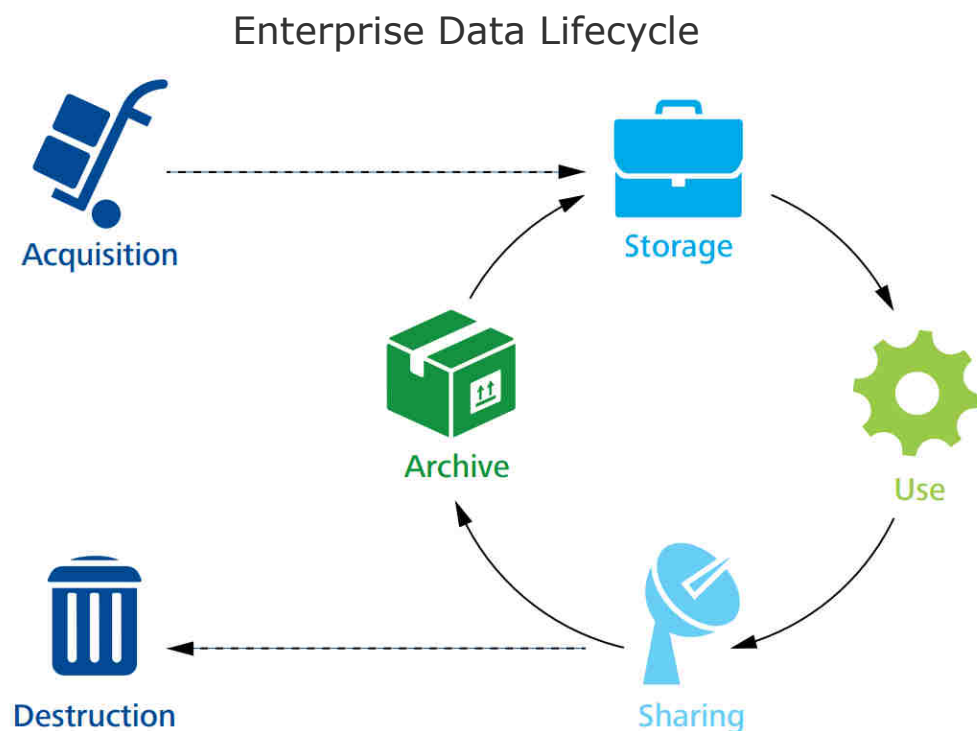
Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident



Private and C

What is Data Leakage?



*Data Leakage is the **movement** of an **information asset** from an **intended state** to an **unintended, inappropriate or unauthorized state**, representing a **risk** or a potentially **negative impact** to the organization.*

Why and How Data Loss Can Happen To Your Organisation?

Because it flows ...

Sensitive data such as **personal information**, **financial data**, and **intellectual property** moves horizontally **across organizational boundaries**, including vertical business processes (e.g., order fulfilment process).

Data in use – What is the agent doing with it?

- Disgruntled or terminated employees copying files containing personal or confidential information to portable devices (e.g., flash drives)
- Users printing sensitive data to equipment in common areas which can be accessed by others

Data in motion – Where is the data going?

- Users sending sensitive data to personal webmail accounts in order to work at home
- Personal and confidential information being shared with third parties for valid business purposes using insecure transmission protocols
- Malicious insiders transmitting personal and confidential information outside of an organizations network

Data at rest – Where is sensitive data located?

- Business users innocently placing personal information in insecure storage locations where access is not administered by IT
- Database administrators storing backup copies of sensitive data in unapproved locations

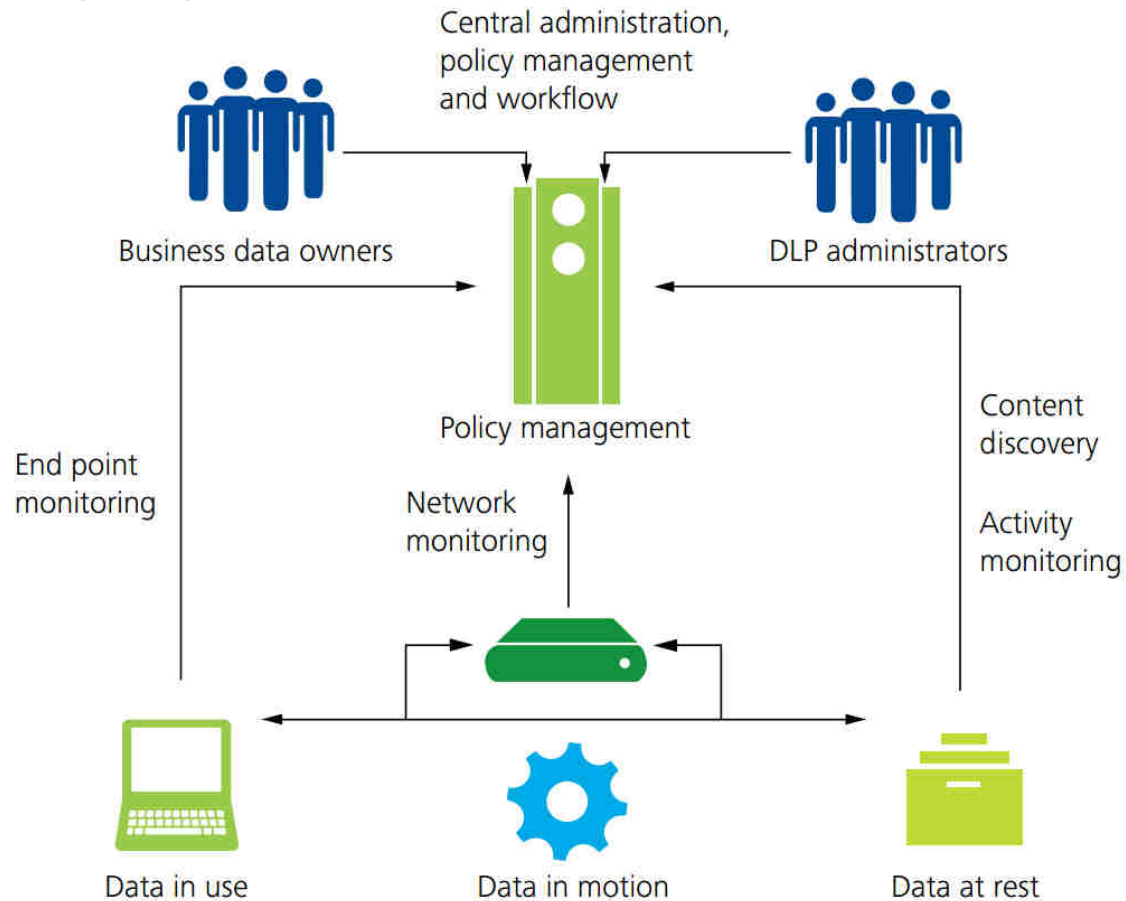


แนวทางการป้องกัน เผื่อระวัง และตอบสนองต่อภัย ทางไซเบอร์

ภาพรวมของการป้องกัน

(Overview of Data Loss Prevention: DLP)

ภาพรวมของแนวทางในการป้องกัน Deloitte's DLP in action



Source: Do you DLP? Maximising the business value of your Data Loss Prevention (DLP) solution, Deloitte

แนวทางการป้องกัน ฝ้าระวัง และตอบสนองต่อภัย ทางไซเบอร์

การฝ้าระวังและตรวจจับ

(Monitoring and Detection)

ตัวอย่างของวิธีการเฝ้าระวัง และตรวจจับ Know Your Employees: KYE

Using **Analytics** and **Discovery** technology, a company can develop **employee's profile** from available input such as:

- Activity logs
- Usage behaviour log
- Data usage logs.

Activity logs:

- Email, Chat
- Phone communication
- Internet browsing history
- PC and Network activity log
- Physical movement

Usage behaviour:

- Time spent on applications and software
- Time of day at which applications and software are used

Data usage logs

- User of external drives
- Copied, moved and/or deleted data

Employee profiling

Employee profile can be compared against **norm** or **peers** and identify **suspicious patterns** of potential abuse. The company may be able to **detect data breach or leakage earlier**.

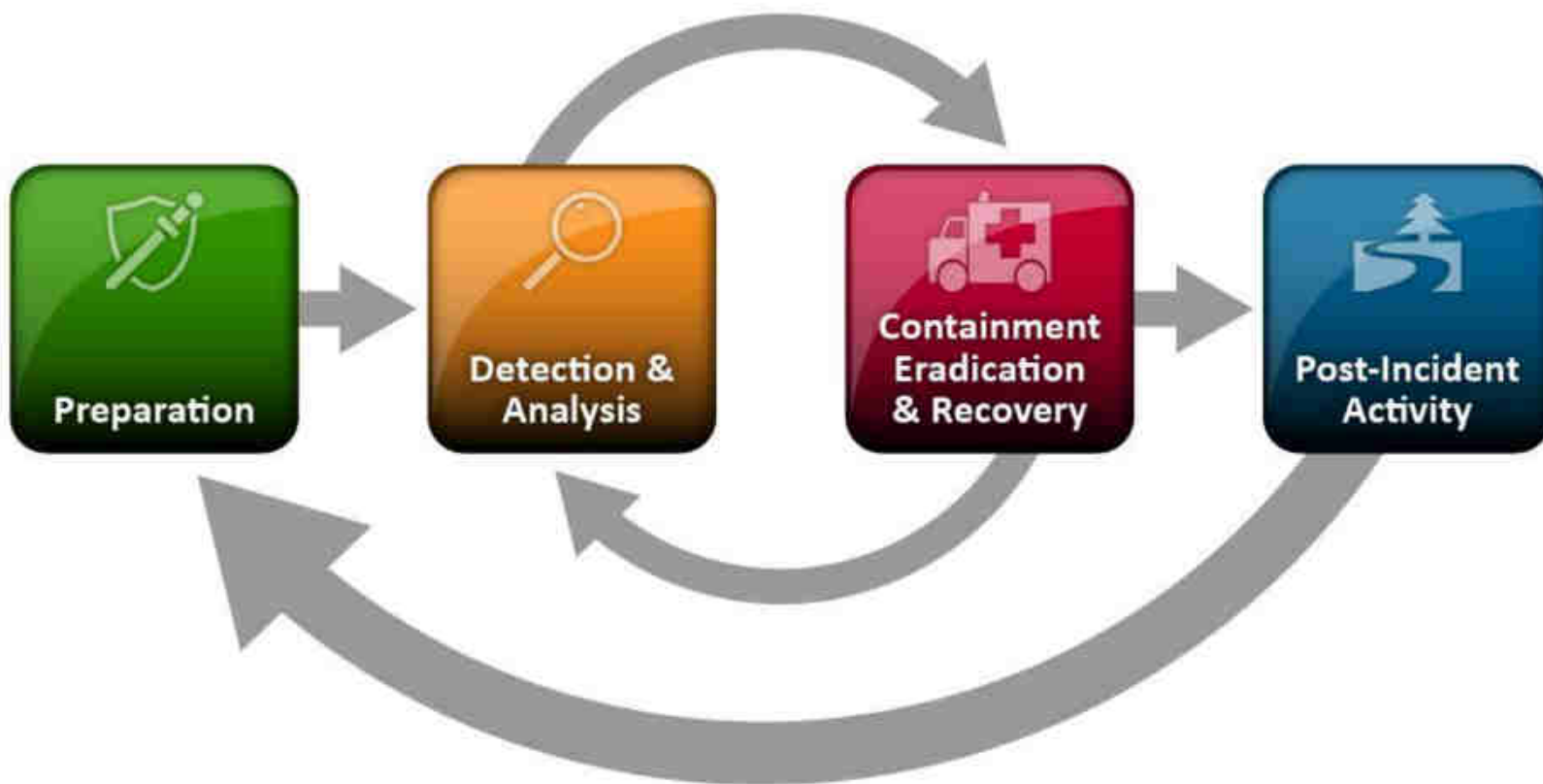
แนวทางการป้องกัน ฝ้าระวัง และตอบสนองต่อภัย ทางไซเบอร์

การตอบสนอง

(Cyber Forensic & Incident Response)

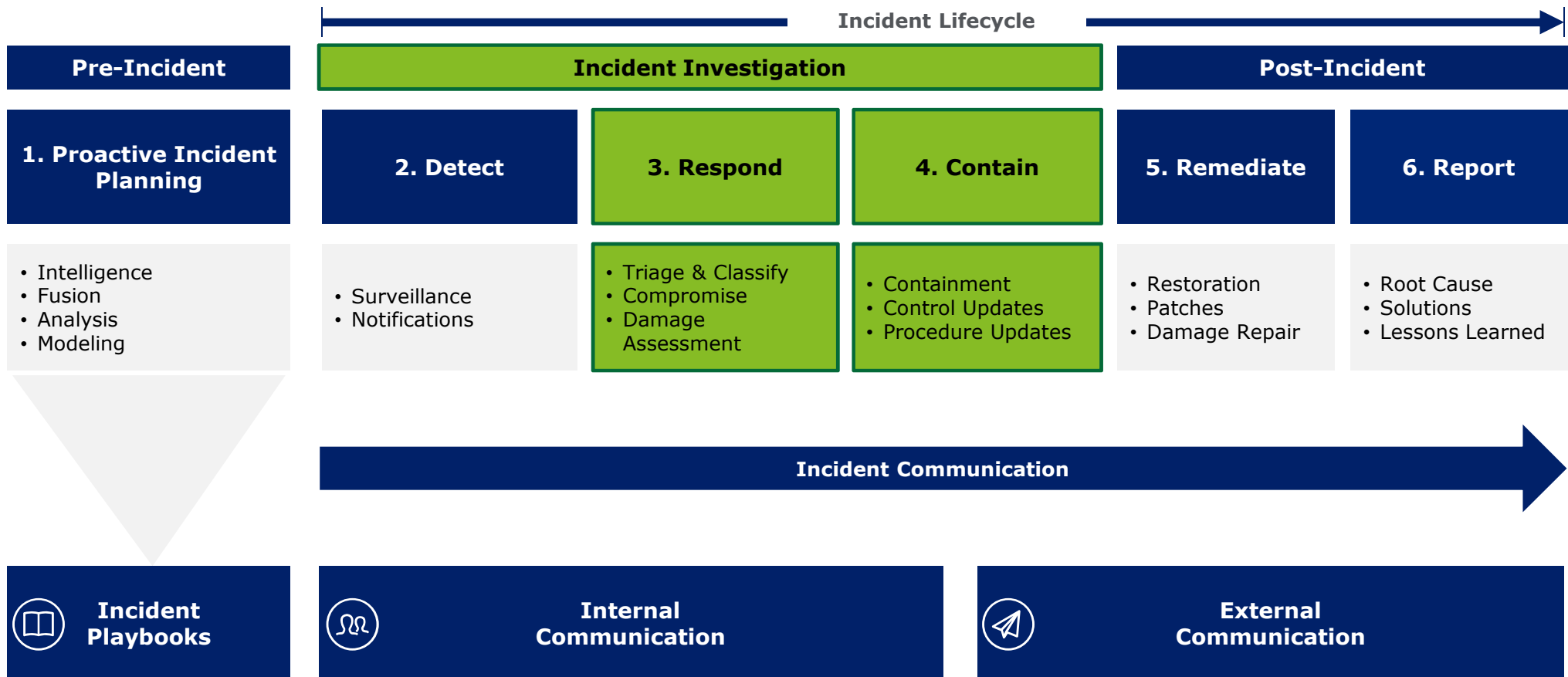
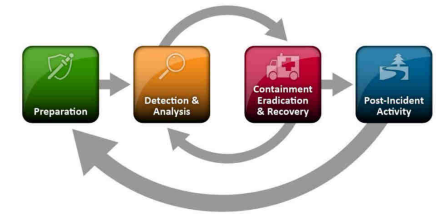
NIST Special Publication 800-61 Revision 2

Computer Incident Handling Guide – The Incident Response Life Cycle



Cyber Forensic

Critical steps in incident response process





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/th/about to learn more about our global network of member firms.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax & legal and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Southeast Asia

Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising approximately 330 partners and 8,000 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Thailand

In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.