Deloitte.

บทเรียนจากกรณีภัยไซเบอร์ที่เกิดขึ้นบ่อยครั้งในองค์กร

Case Studies related to Data Security and Protection

14 August 2018

Forensic

Private and Confidential

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

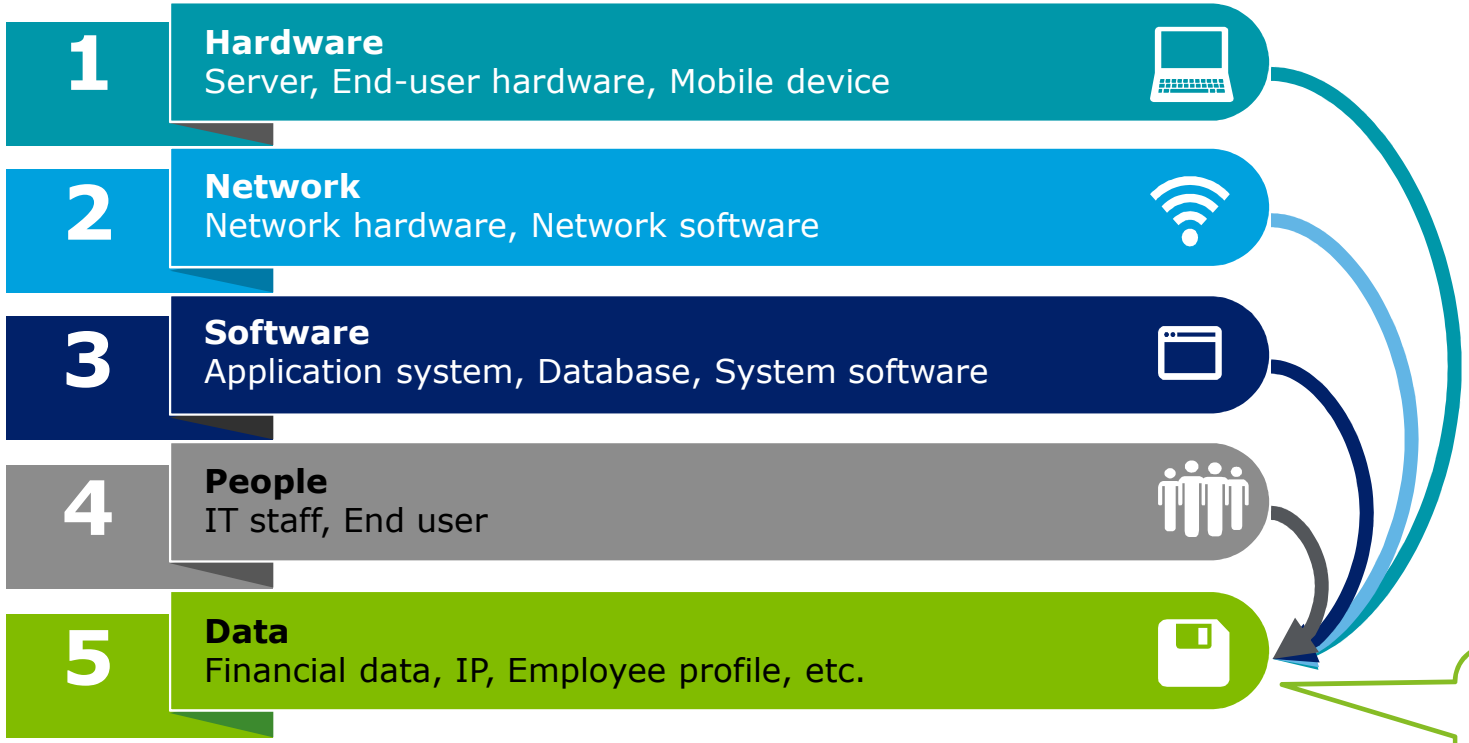
About Deloitte Forensic

Why do we show up in a Cyber crisis?

ภัยไซเบอร์ที่เกิดขึ้นบ่อยครั้งในองค์กร

แนวโน้ม และผลกระทบ

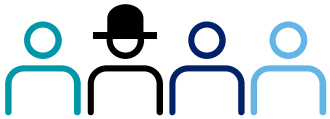
องค์ประกอบด้านเทคโนโลยีในองค์กร และภัยคุกคามในรูปแบบต่าง ๆ



- *Physical damage / Loss / Theft*
- *Channel of Intrusion and Exfiltration, Catalyst for pervasiveness*
- *Has been overlooked, not properly managed*
- *Is this the most vulnerable?*

- Reputational risk
- Regulatory risk
- Financial risk
- Operational risk

แนวโน้มของภัยคุกคามทางไซเบอร์
The Changing Threat Landscape



- *เกิดได้ทั้งจากบุคคลภายนอก และภายในองค์กร*
- *บุคคลภายในองค์กรที่กระทำการไปโดยไม่ได้มีเจตนานั้น ถือเป็นปัญหาหลักขององค์กร*
- *การสร้างความรู้ความตระหนัก ผ่านการฝึกอบรม ตามบทบาทหน้าที่จะช่วยลดความเสี่ยงลงได้*

- *การเข้าถึงโดยมิชอบ และการเปิดเผยข้อมูลความลับขององค์กร หรือข้อมูลส่วนบุคคลถือเป็นแนวโน้มภัยคุกคามที่สำคัญ*
- *องค์กรต่าง ๆ ควรมีมาตการในการเก็บรักษาข้อมูลสำคัญขององค์กร ที่เป็นไปตามมาตรฐานสากล และเป็นไปตามข้อกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล*
- *มีการตรวจสอบมาตรฐานความปลอดภัยดังกล่าวอย่างสม่ำเสมอ*

Source: IBM X-Force Threat Intelligence Index 2018

แนวโน้มของภัยคุกคามทางไซเบอร์
The Changing Threat Landscape

- *ภัยคุกคามจากซอฟท์แวร์เรียกค่าไถ่ **(Ransomware)** และการทำลายข้อมูล **(Data-wiping attacks)** ยังคงมีเป็นหนึ่งในแนวโน้มที่สำคัญ*
- *ภัยคุกคามในรูปแบบดังกล่าว สร้างผลกระทบต่อการดำเนินงานสร้างความเสียหายทั้งในทางการเงิน และความน่าเชื่อถือขององค์กร*

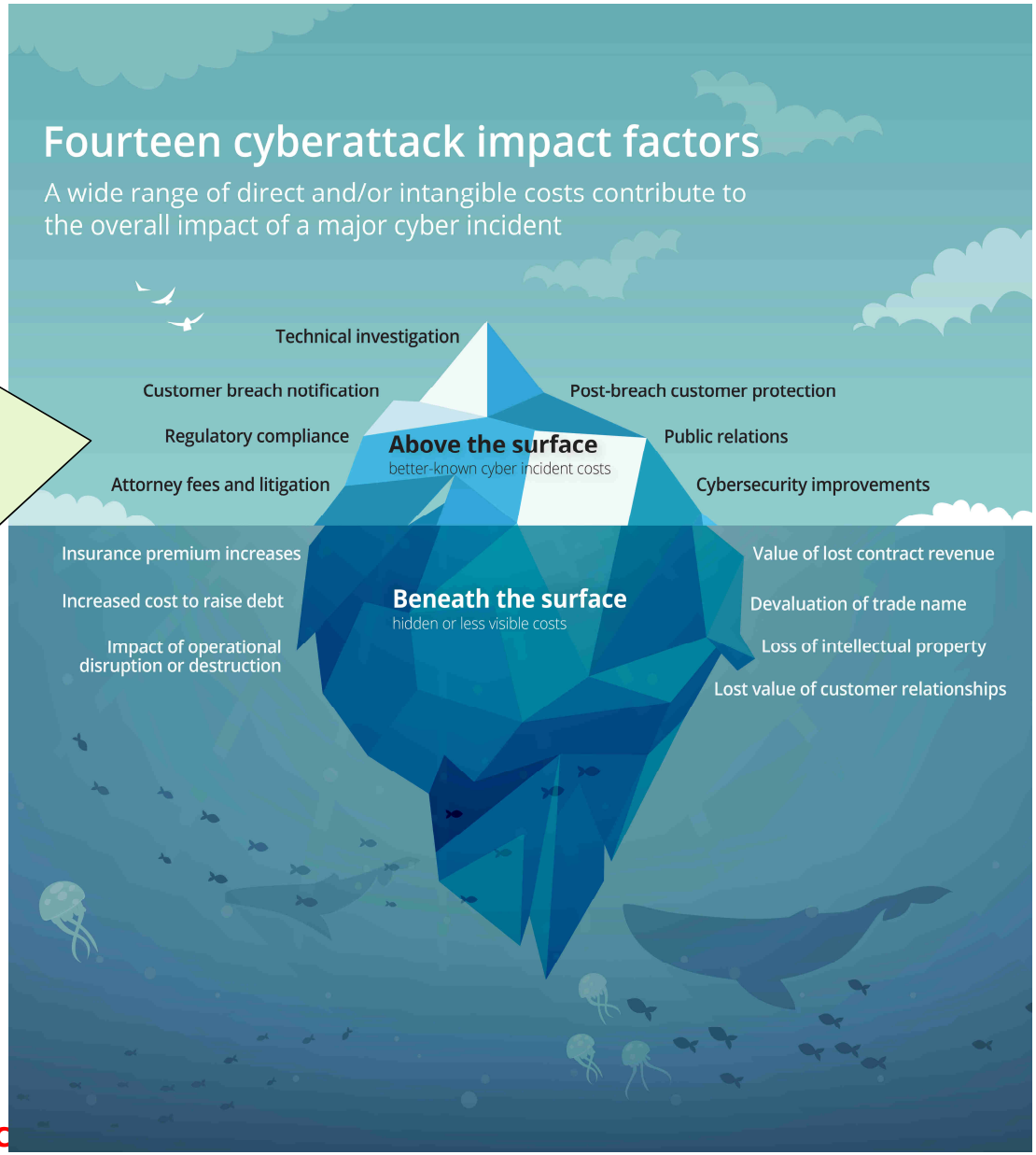
- *แนวทางการป้องกันที่สำคัญยังคงเป็นเรื่องพื้นฐาน เช่น การติดตั้งตัวปรับปรุงหรือแก้ไขระบบ **(Patch management)** ทั้งในส่วนของ **Hardware** และ **Software***
- *การนำเอาระบบการตรวจตรา **(Monitoring system)** แบบ **Real-time** รวมทั้งการใช้ปัญญาประดิษฐ์ **(AI, Machine learning)** มาใช้ในการตรวจจับรูปแบบที่ต้องสงสัย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

Source: IBM X-Force Threat Intelligence Index 2018

ความเสียหายจากภัยคุกคามทางไซเบอร์
Beneath the Surface of a Cyberattack

ค่าใช้จ่าย หรือ ความเสียหายที่เห็นได้ชัดเจน

- *การสืบสวนสอบสวน*
- *การแจ้งเตือนลูกค้าที่ได้รับผลกระทบ*
- *การป้องกันและรักษาผลประโยชน์ลูกค้าที่ได้รับผลกระทบ*
- *การปฏิบัติตามข้อกฎหมายต่าง ๆ*
- *การสื่อสารกับสาธารณชน*
- *การดำเนินคดี หรือ การเกิดข้อพิพาทต่าง ๆ*
- *การปรับปรุงความมั่นคงปลอดภัยไซเบอร์*

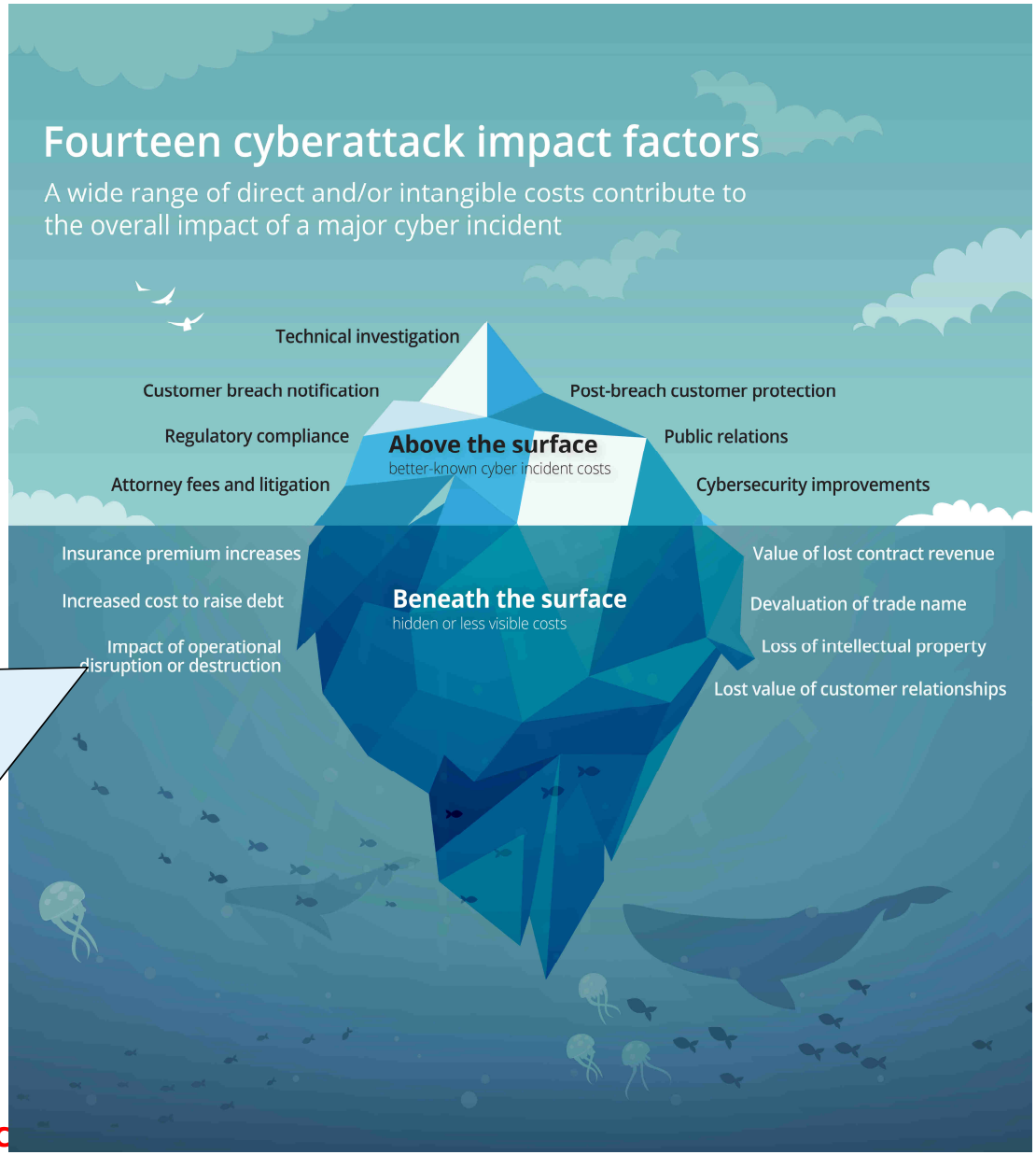


Source: Beneath the surface of a cyberattack, Deloitte

ความเสียหายจากภัยคุกคามทางไซเบอร์
Beneath the Surface of a Cyberattack

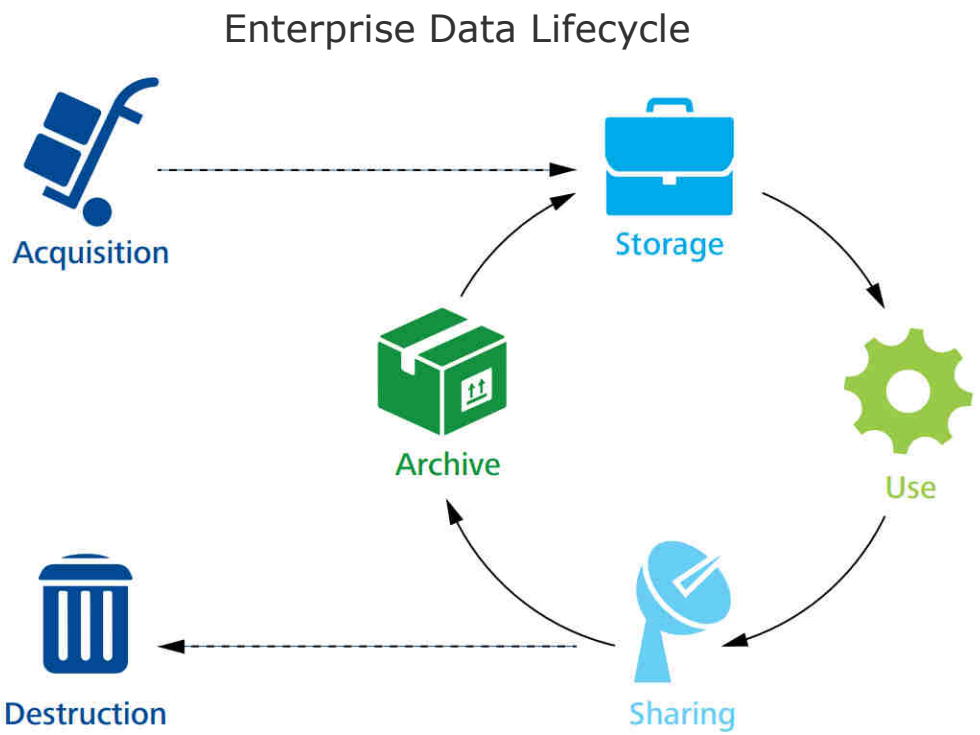
ค่าใช้จ่าย หรือ ความเสียหายที่ซ่อนอยู่

- *เบี้ยประกันภัยทางไซเบอร์ที่สูงขึ้น*
- *มูลค่าของสัญญาทางธุรกิจที่สูญเสียไป*
- *ชื่อเสียงและความน่าเชื่อถือที่ลดลง*
- *ต้นทุนในการหาสินเชื่อใหม่ที่สูงขึ้น (อันเนื่องมาจากความน่าเชื่อถือที่ลดลง)*
- *ผลกระทบจากการปฏิบัติงานที่หยุดชะงักหรือถูกทำลาย*
- *การสูญเสียทรัพย์สินทางปัญญา*
- *การสูญเสียความสัมพันธ์กับลูกค้า*



Source: Beneath the surface of a cyberattack, Deloitte

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

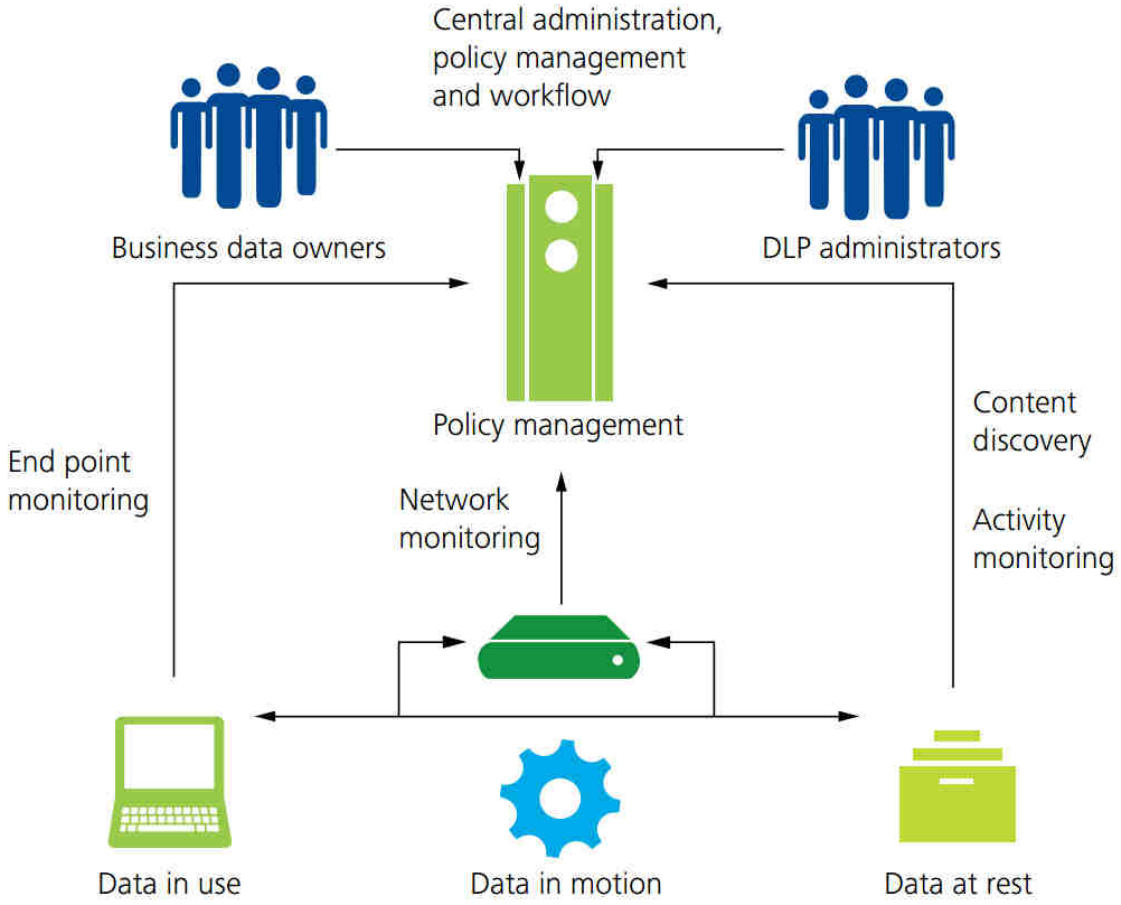
Data at rest – Where is sensitive data located?

- 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 เฝ้าระวัง และตอบสนองต่อภัยทางไซเบอร์

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 เฝ้าระวัง และตอบสนองต่อภัยทางไซเบอร์

การเฝ้าระวังและตรวจจับ
(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.*

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

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

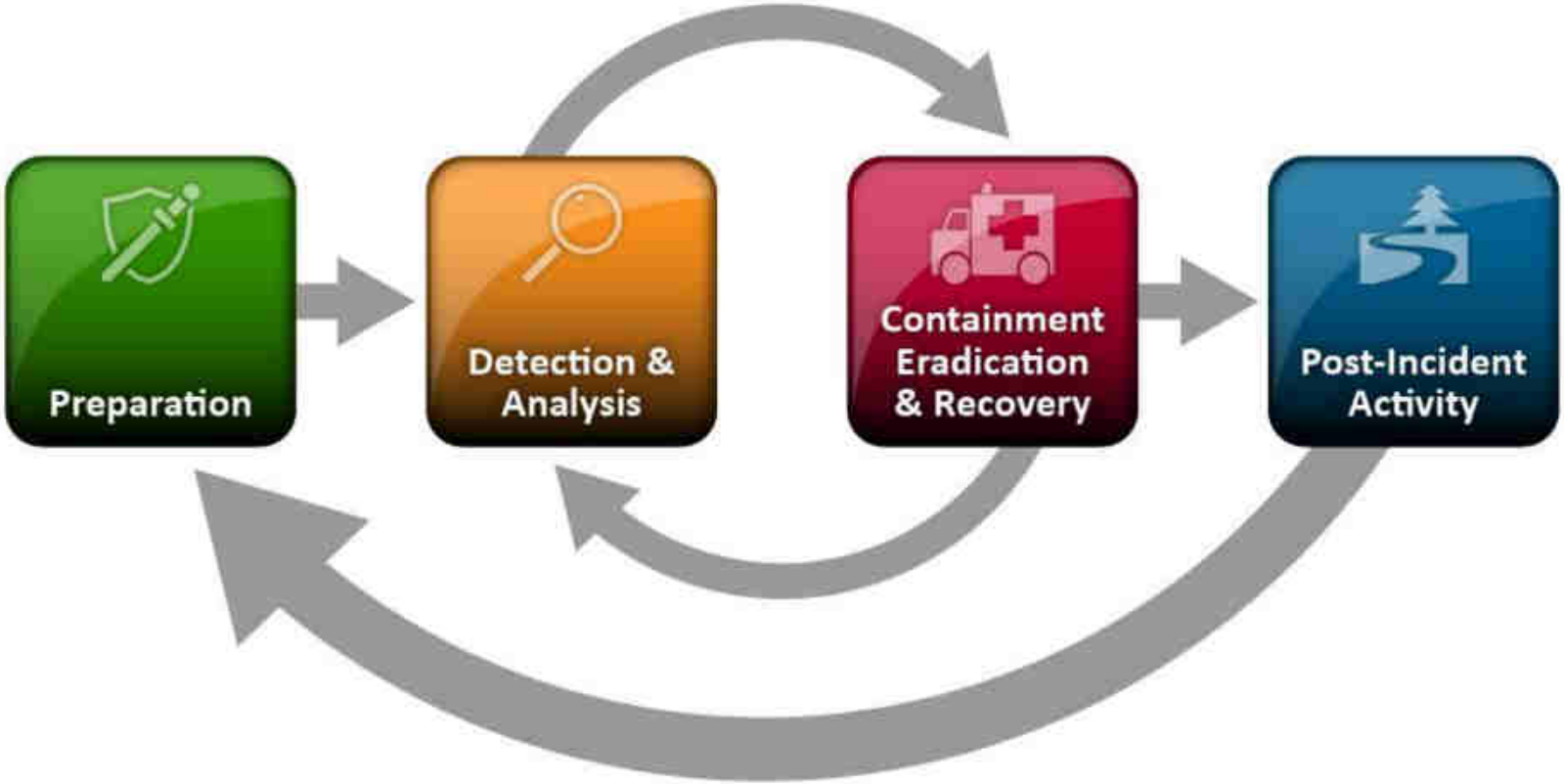
Data usage logs
- User of external drives
- Copied, moved and/or deleted data

แนวทางการป้องกัน เฝ้าระวัง และตอบสนองต่อภัยทางไซเบอร์

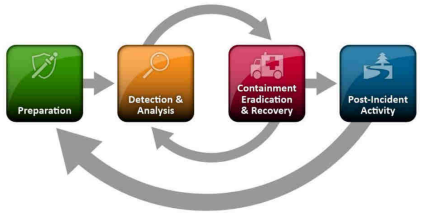
การตอบสนอง
(Cyber Forensic & Incident Response)

NIST Special Publication 800-61 Revision 2

Computer Incident Handling Guide – The Incident Response Life Cycle



Cyber Forensic
Critical steps in incident response process



Incident Lifecycle

Pre-Incident	Incident Investigation			Post-Incident	
1. Proactive Incident Planning	**2. Detect**	**3. Respond**	**4. Contain**	**5. Remediate**	**6. Report**
• Intelligence • Fusion • Analysis • Modeling	• Surveillance • Notifications	• Triage & Classify • Compromise • Damage Assessment	• Containment • Control Updates • Procedure Updates	• Restoration • Patches • Damage Repair	• Root Cause • Solutions • Lessons Learned

Incident Communication

Incident Playbooks	**Internal Communication**	**External Communication**

Deloitte.