Deloitte.

Cyber Incidents – Data leakage

Case Study & Lesson Learnt

23 May 2018

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.

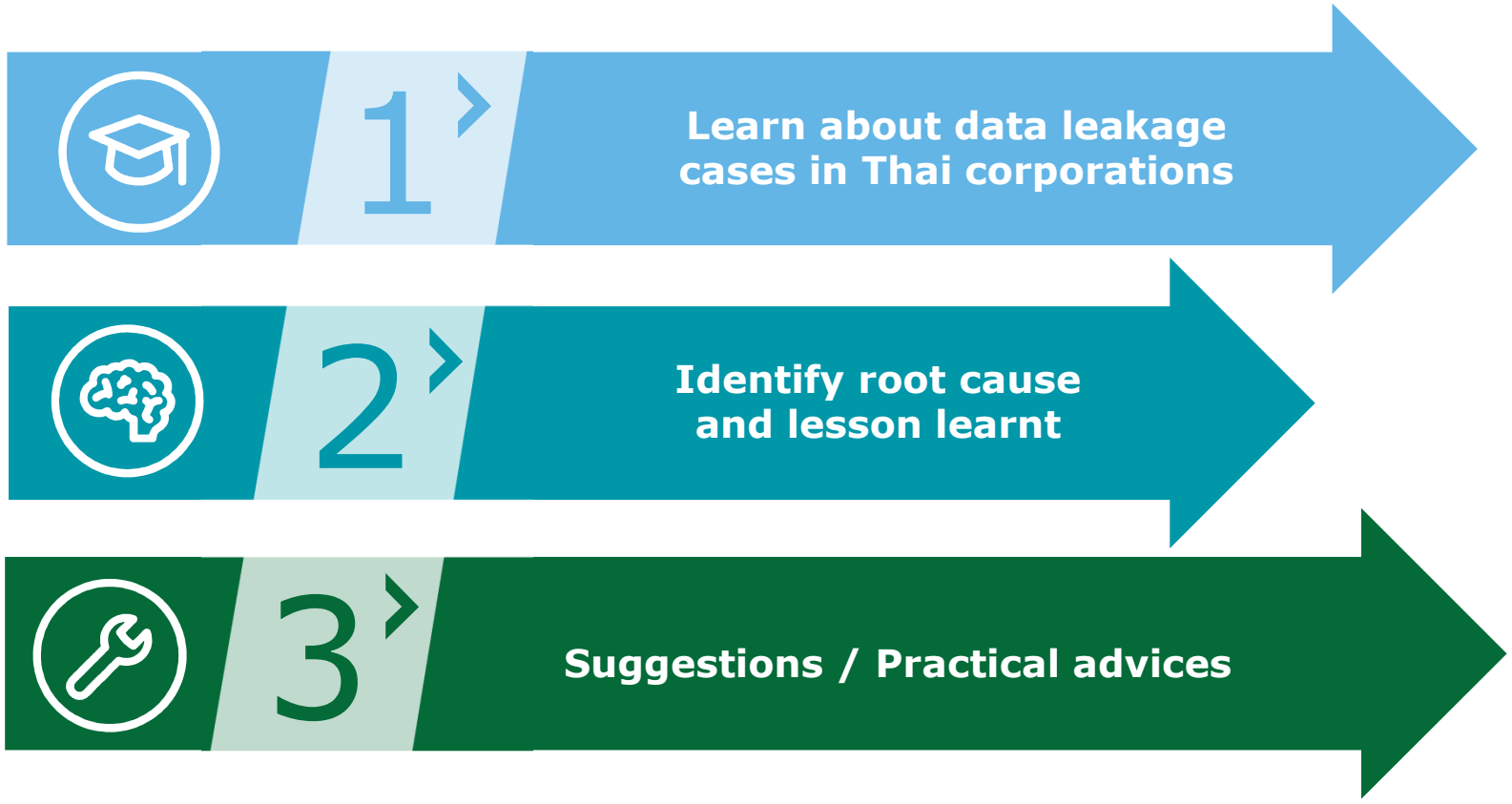
In addition, the Material is limited by the time available and by the information made available to us. You should not consider the Material as being comprehensive as we may not become aware of all facts or information. Accordingly, we are not in a position to and will not make any representation as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

Key objectives

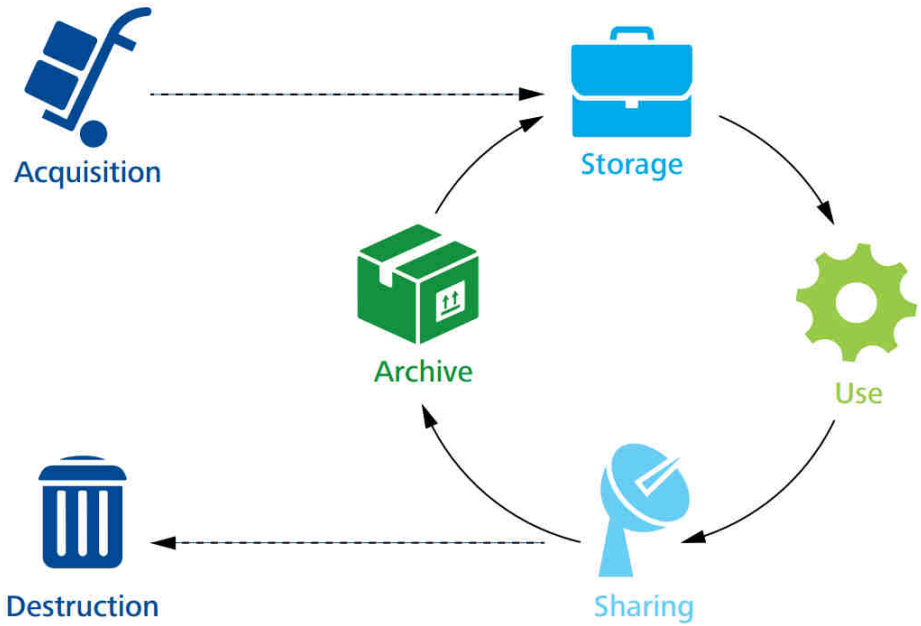
What you can expect from this session



What is Data Leakage?

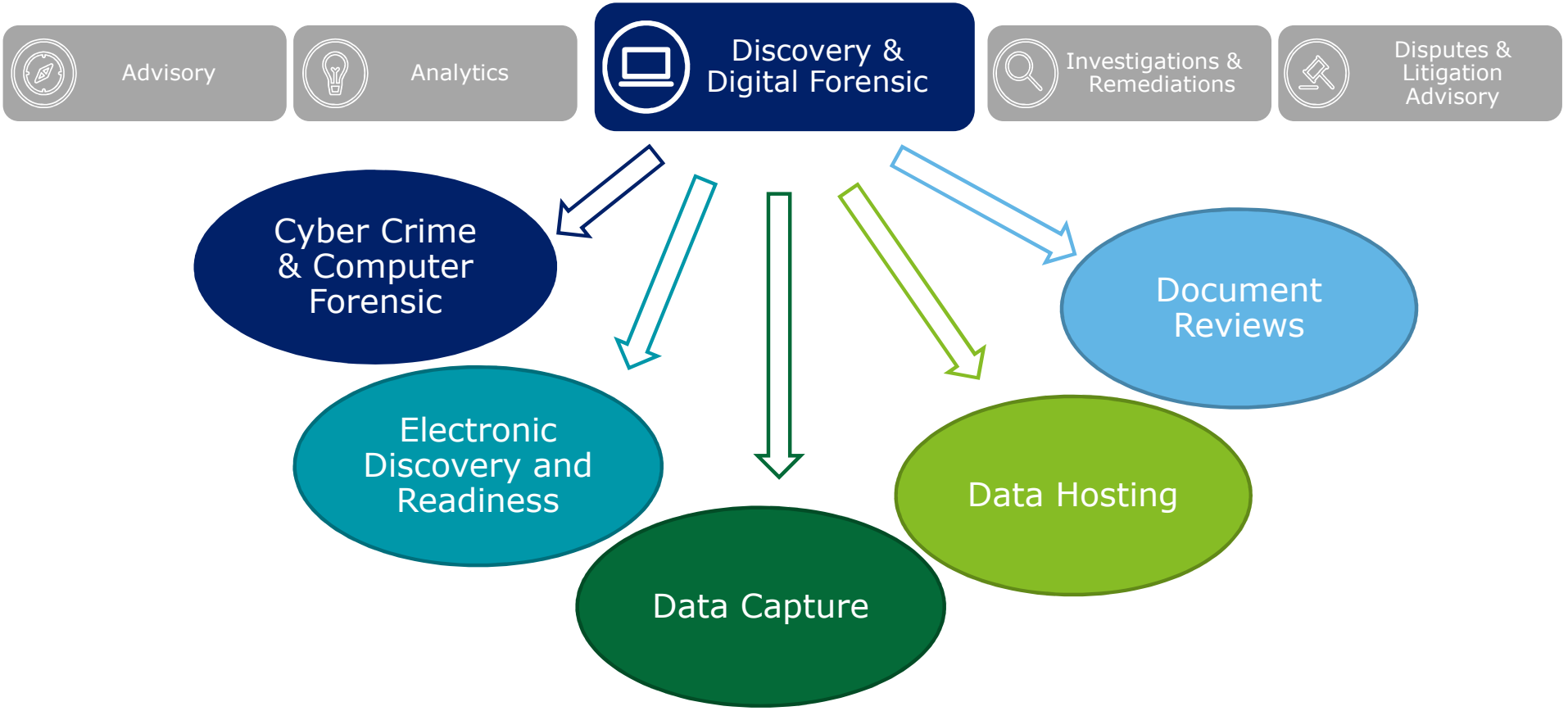
*The **movement** of an **information asset** from an **intended state** to an **unintended, inappropriate or unauthorized state**, representing a **risk** or a potentially **negative impact** to the organization.*

Enterprise Data Lifecycle



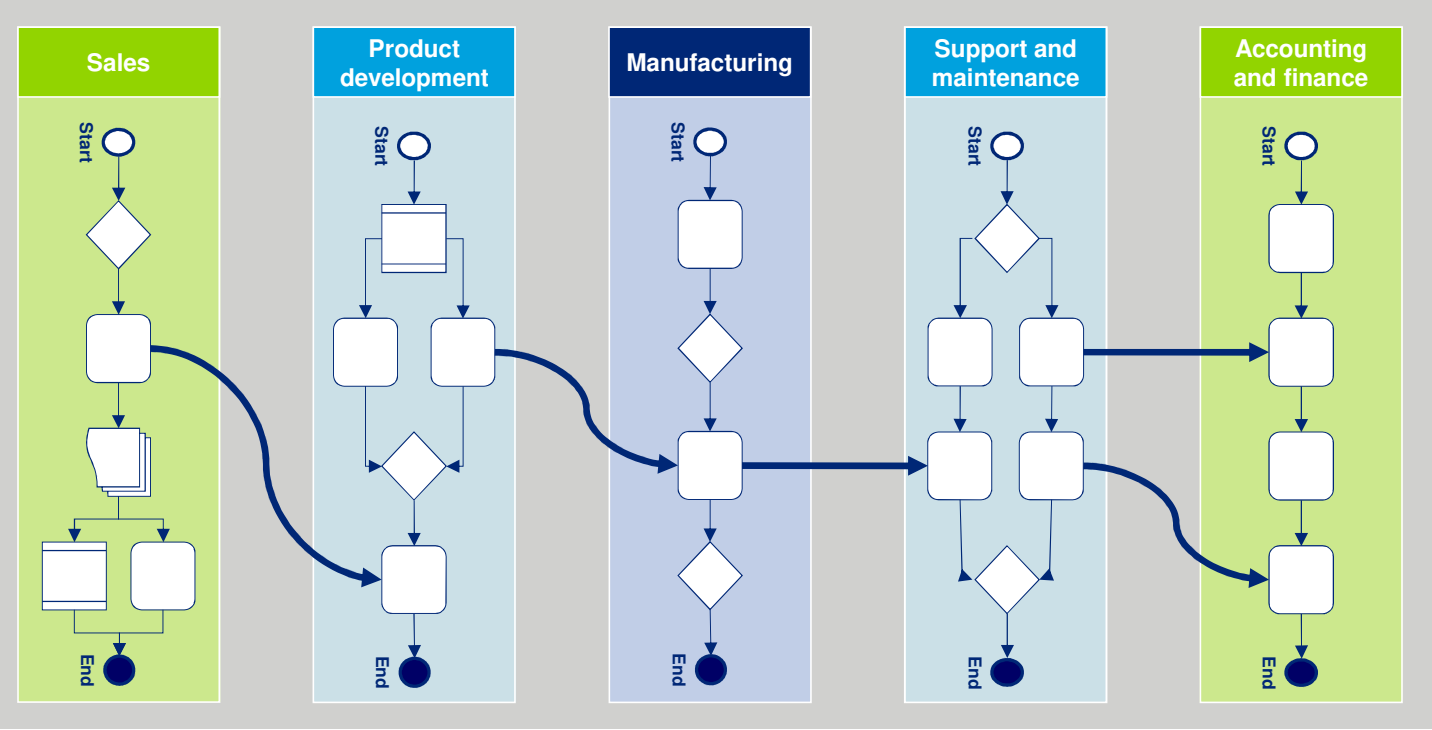
Deloitte Discovery

Why do we show up at a crisis?



Why could data leak?

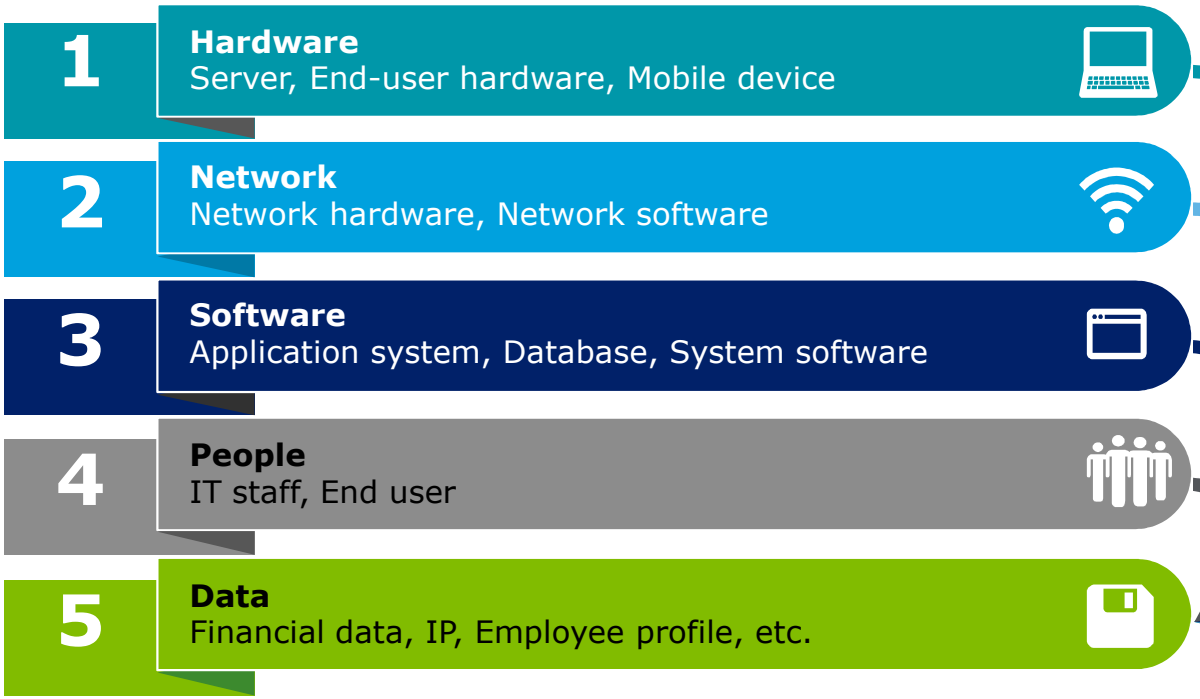
Because it flows …



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).

Technology elements in the business

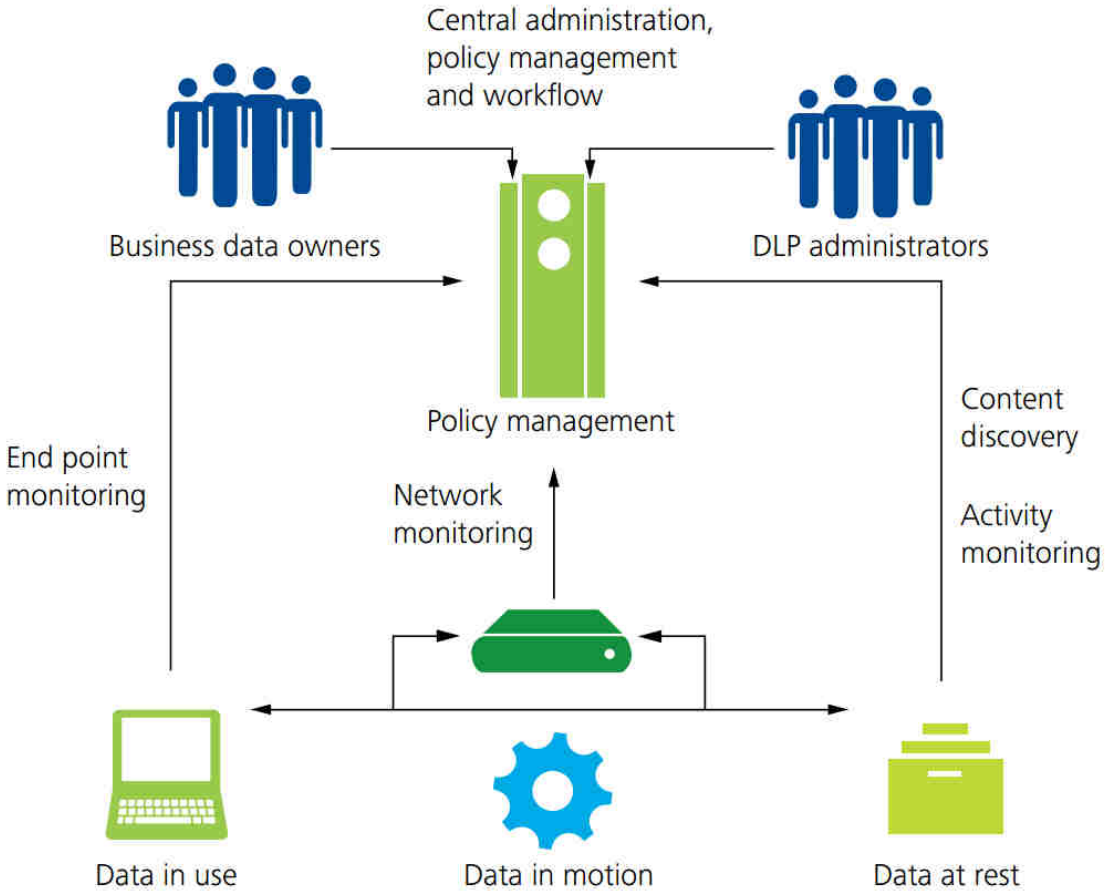
And why they can lead to data leakage



- *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

Deloitte’s DLP in Action



Key Considerations

To assess your data leakage risks

General

- What **information or data elements** present the **most risk**?
- What **locations or business units** present the **most risk**?
- What are our **mitigating controls**?
- How **robust** of a **governance structure** and **incident response workflow** do we need to support our goals and mitigate our risks?
- What type of **resourcing** do we need to **support management** of the tool and the **incidents it generates** on an on-going basis?

Data-at-rest

- What **types of data repositories** does the solution need to be able to scan?
- What do we plan to **do with the data** once it is found?

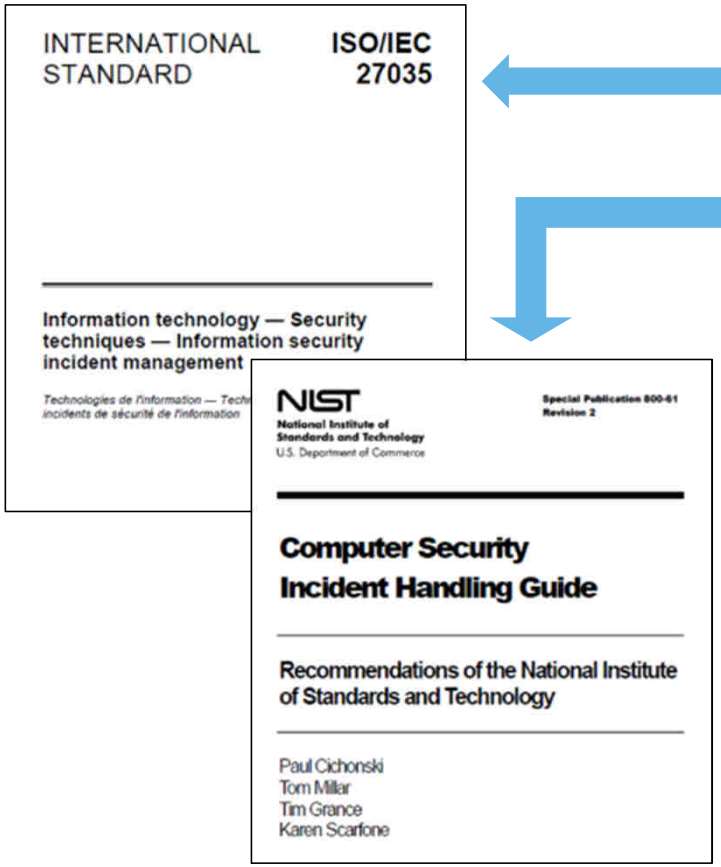
Data-in-motion

- Do we care about **outgoing** transmissions only, or **incoming and internal** as well?
- What **protocols** do we need to monitor and protect?
- Do we need to **block or encrypt** traffic?

Data-in-use

- What **platforms** does the solution need to support?
- What do we want the tool to accomplish when users are **not on the network**?

Examples of guidelines from recognized institutes



ISO/IEC 27035:2016 – Information technology incident management

NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide

SANS institute – Various contents …

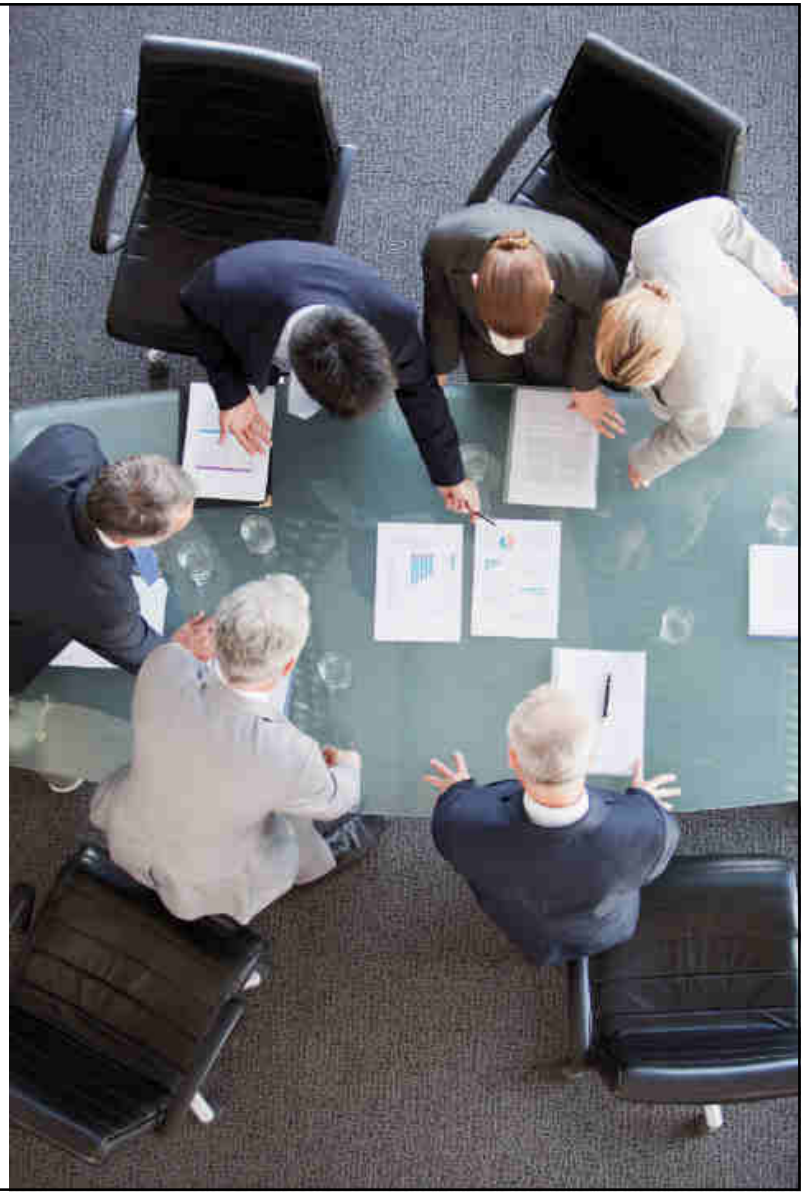
And many more from other organizations…

- https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response
- https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

IT Asset Management (ITAM)

Efficient ITAM could mitigate risks on data leakage and help you comply with regulations

- **Detailed inventory of IT assets** could help data controllers analyze their current IT resources used to process personal data and asses the risk of data breach.
- **Appropriate internal controls** or counter measure could be implemented to mitigate data breach risk.
- In case of data breach, ITAM will **help the data controllers/processors notify the regulators** by answering their questions such as:
  - What assets/data were affected?
  - Who was affected? Who had the access to the assets?
  - Where was the affected assets located? Where was the data processed?
  - How will data controller response to the breach? How many stakeholders were affected?
- Overall, ITAM could help data controllers **understand their IT landscape, optimize IT costs and provide a foundation for complying to regulations**.



Contact

Thanwa Wathahong
Director – Deloitte Forensic
twathahong@deloitte.com

Thanwa is a Director at Deloitte Forensic practice in Thailand. He focuses on Digital and Cyber forensics, Discovery and Corporate Investigation, Forensic Analytics, Cyber incident response, Business Intelligence, Anti-Bribery & Corruption, Fraud Risk Management, Litigation Support & Dispute Analysis, and Fraud Detection, Monitoring and Fraud Management System.

He holds two bachelor's degrees; in Computer Engineering and Law, plus MBA in Finance.

He is also:
- *A guest lecturer in Fraud Analysis and Detection at the Master of science program in Cyber security and information assurance (international program), Mahidol University*
- *A trainer at Federation of Accounting Professions, Thailand.*

Deloitte.