

DEEP DIVE

# DIGITALLEGAL ACADEMY 2024

by TaylorWessing

## Cybersecurity Reloaded # 2: Responding to Cyber Incidents

Dr. David Klein (Taylor Wessing), Eric M. Robinson, Zoran Zovko (KLDDiscovery)



# Agenda

1 Introduction

---

2 The legal perspective – quick recap


---

3 The legal perspective – consequences

---

4 Supportive technical solution

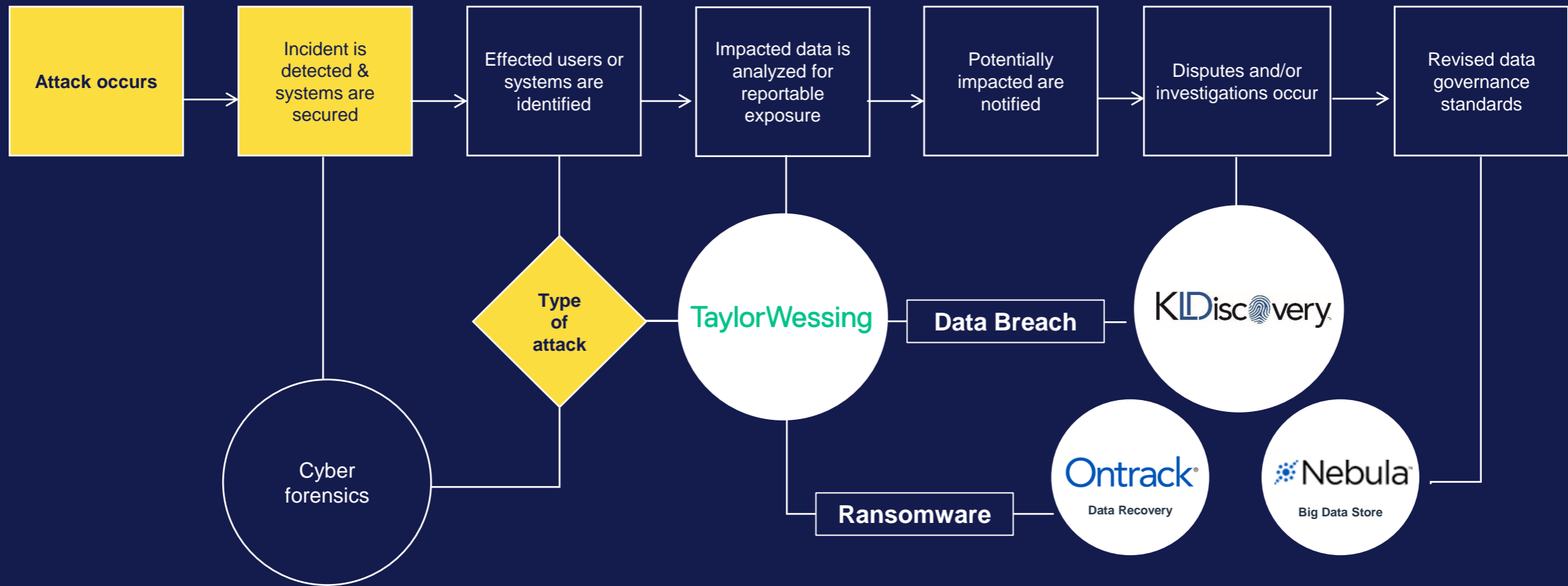
---

 If you take anything away from this discussion, it should be this:

*An integrated approach to governing privacy, security, and compliance is essential for managing risk in the modern threat environment. Collaboration and alignment should be core strategic imperatives.*

# Responding to Cybersecurity Incidents

## Critical functions in the wake of a cyber attack



# ➤ Every Major Industry is Impacted

Post-breach impact assessments and related discovery arises across a broad spectrum

## Financial Services

- Banking
- Accounting
- Real Estate
- Mortgage Services

## Health Care

- Hospital systems
- Managed Care
- Health Insurance
- Benefits Administration
- Doctors

## Technology

## Insurance

## Legal Services

## Life Sciences

- Pharmaceutical
- Medical Device

## Higher Education

## Retail

DEEP DIVE

DIGITAL LEGAL >  
ACADEMY 2024

by TaylorWessing



# The legal perspective

quick recap

# Small list of duties

NIS2	NIS-2 National Laws	RL	WKRL	GeschGehG
Cyber Resilience Act (CRA)	KRITIS	DORA	DIRL	IT-Sicherheitsgesetz
Cybersecurity Act	DMA	BDSG	GDPR	RED
Data Act	AI Act	KI-HaftungsRL	DGA	Maschinenverordnung
EHDS	GDNG	eIDAS2-VO	DSA	Chips Act

# Small list of duties

## Today's focus

NIS2	NIS-2 National Laws	RL	WKRL	GeschGehG
Cyber Resilience Act (CRA)	KRITIS	DORA	DIRL	IT-Sicherheitsgesetz
Cybersecurity Act	DMA	BDSG	GDPR	RED
Data Act	AI Act	KI-HaftungsRL	DGA	Maschinenverordnung
EHDS	GDNG	eIDAS2-VO	DSA	Chips Act



# ➤ Data Breach & GDPR

## personal data breach

*[...] means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*

Art. 33 GDPR

### Notification obligation to the competent authorities

Within 72h

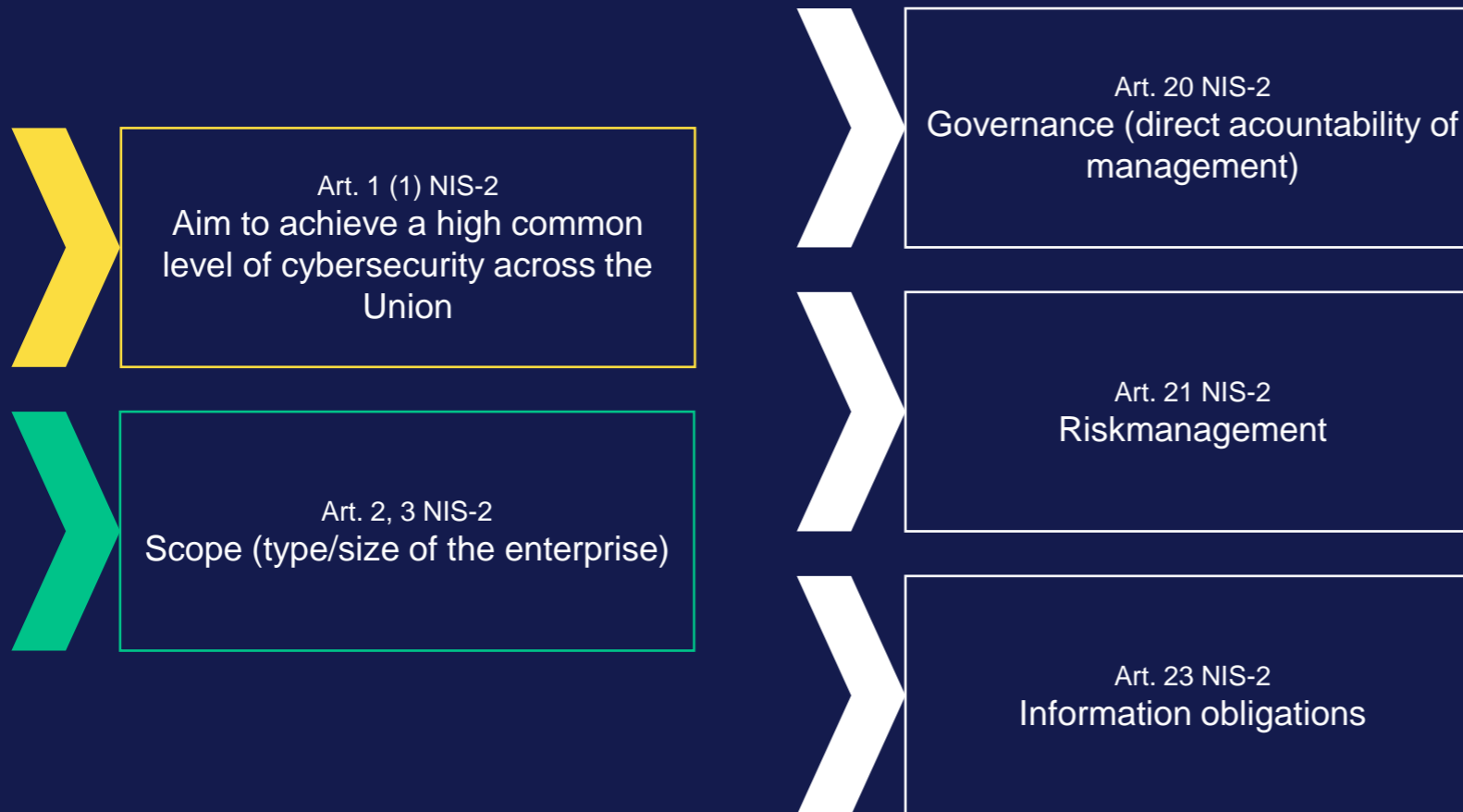
Mandatory content of the notification

Art. 34 GDPR

### Information of data subjects

In case of high risk for data subjects

# Obligations due to NIS-2



# Data Breach & NIS-2

## Significant incident

*“incident” means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.*

*Incident is regarded significant if*

- a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;*
- b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.*

Art. 23 (4) lit. a) NIS-2

### **Early warning to the competent authority/authorities**

Within 24h

Art. 23 (4) lit. b) NIS-2

### **Incident notification to the competent authority/authorities**

Within 72h

Initial assessment (severity & indicators of compromise)

Art. 23 (4) lit. d) NIS-2

### **Final report**

Within one month

Comprehensive information about the incident

## ➤ What else?

➤ Art. 17 MAR  
Ad-hoc Information

➤ Information to Cyber-Insurance

➤ Further notification obligations to authorities

➤ Damage claims of data subjects & contract partners

➤ Fines

➤ § 129 (1) 2 StGB  
Support of a criminal group

DEEP DIVE

DIGITAL LEGAL >  
ACADEMY 2024

by TaylorWessing



# The legal perspective

consequences



# Consequences

Art. 33 GDPR

## **Notification obligation to the competent authorities**

Within 72h

Mandatory content of the notification

- Full forensic report required (what has happened)
- Full assessment of personal data/data subjects involved required for information obligations (Art. 34 GDPR)



# Consequences

Art. 34 GDPR

## **Information of data subjects**

In case of high risk for data subjects

- Full assessment of personal data/  
data subjects involved required
  - Risk assessment
- Identification of data subjects

# Consequences

Art. 23 (4) lit. a) NIS-2

## **Early warning to the competent authority/authorities**

Within 24h

Art. 23 (4) lit. b) NIS-2

## **Incident notification to the competent authority/authorities**

Within 72h

Initial assessment (severity & indicators of compromise)

- Full forensic report required (what has happened)
- Full assessment of incident with risk assessment

Art. 23 (4) lit. d) NIS-2

## **Final report**

Within one month

Comprehensive information about the incident



# Consequences

Art. 17 MAR  
**Ad-hoc Information**

**Information to  
Cyber-Insurance**

**Further notification  
obligations to authorities**

- Full forensic report required (what has happened)
- Full assessment of incident with risk assessment

# Consequences



## Fines

- Full forensic report required (what has happened)
- Full assessment of incident with risk assessment



# Consequences

DEEP DIVE

DIGITALLEGAL  
ACADEMY 2024

by TaylorWessing

**Damage claims of data  
subjects & contract  
partners**

- Full forensic report required (what has happened)
- Full assessment of incident with risk assessment
  - Restoration of data

DEEP DIVE

DIGITAL LEGAL >  
ACADEMY 2024

by TaylorWessing



**Supportive technical solution**

# Key Components of a Cybersecurity Program

1. **Leadership buy-in.** Obtain executive support and sponsorship to prioritize security.
2. **Risk assessments.** Continuously identify, analyze and prioritize cyber risks to the organization.
3. **Written Policies and procedures.** Establish and implement policies for key such as access controls, data protection and IR.
4. **Awareness training.** Educate employees on cybersecurity best practices and how to identify threats.
5. **Network security.** Use firewalls, intrusion detection/prevention systems and segmentation to protect networks.
6. **Endpoint security.** Deploy antivirus/ antimalware tools, patch management and device controls.
7. **Access controls.** Manage access to systems and data via identity and access management.
8. **Vulnerability management.** Regularly scan for and patch software/system **vulnerabilities**.
9. **Data security.** Protect sensitive data at rest and in transit through encryption and tokenization.
10. **Incident response plan.** Have an IR plan and team in place to quickly detect, respond to and recover from incidents.

# What does it take to make a cybersecurity program successful?

- Leadership commitment
- Risk assessments
- Policies and procedures
- Training and awareness
- Oversight and auditing
- Incident response planning
- Third-party management
- Continuous improvement
- Resource allocation
- Accountability
- Clear communications and reporting channels

**Aligning these programs under a central governance framework allows organizations to efficiently manage overlaps and dependencies between them**

## Cybersecurity Success....

*Requires a layered defense of people, processes and technology controls focused on the most critical assets and risks. Continuous monitoring, training and improvement are key to success.*

# Ediscovery ≠ Data Breach Response Because It:

Is Under-Inclusive

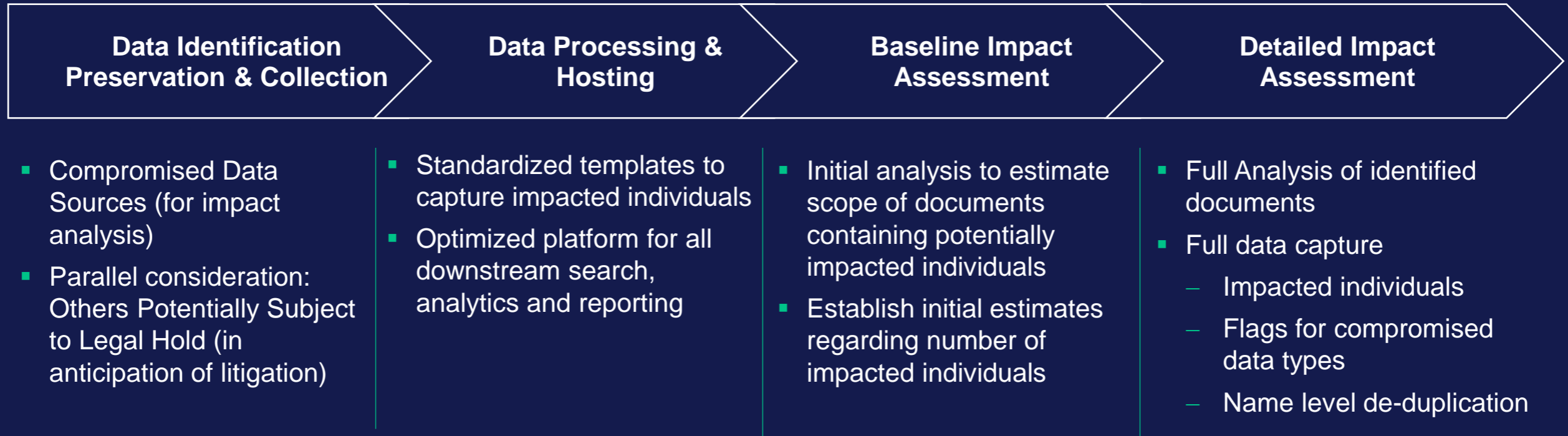
Is Over-Inclusive

Is a Different Kind of “Review”

Is Built Around Docs,  
Not Entities



# Overview of Data Breach Impact Assessment



DEEP DIVE

DIGITAL LEGAL >  
ACADEMY 2024

by TaylorWessing

> Thank you for your attention!

 **Speaker**



**Eric Robinson, JD/PMP**  
**KLDiscovery Ontrack LLC**  
**VP, Global Advisory Services & Strategic Solutions**  
Eric.Robinson@kldiscovery.com



**Zoran Zovko**  
**KLDiscovery Ontrack GmbH**  
**Director, Business Development**  
zoran.zovko@kldiscovery.com



**Dr. David Klein, LL.M. (Univ. of Washington), CIPP/E**  
**Taylor Wessing**  
**Salary Partner**  
d.klein@taylorwessing.com