

hexnode



DATA COMPLIANCE: THE SERIES

**GET IT RIGHT THE FIRST TIME**

Hosted by: Peter Geelen, Edwin Jerald

7 April 2022 | 12 PM CST

## What we'll discuss today

- 1 Introduction
- 2 Data is the new oil...
- 3 Data management essentials
- 4 How to get started in practice
- 5 Some take-aways
- 6 Hexnode and compliance

# About me

<https://www.linkedin.com/in/pgeelen/>

Sustainable secure & safe. Life hacker.  
Anything information security, data  
protection & privacy, cyber & cloud  
security. IAM, trainer & coach.




Peter GEELEN  
ISMS/PIMS Master, cDPO,  
Accredited Lead Auditor  
ISMS/PIMS/BCMS/QMS



A silhouette of an oil pumpjack (jackal) is shown against a clear blue sky at dusk. The pumpjack is a large mechanical device used for extracting oil from a well. It consists of a long walking beam pivoted in the middle to a vertical support. One end of the beam is connected to a long rod that goes down into the well, and the other end is connected to a counterweight. The pumpjack is shown in a position where the counterweight is at its lowest point. The sky is a deep blue, and the ground is dark. The text "Data is the new oil" is overlaid on the image in a white, sans-serif font.

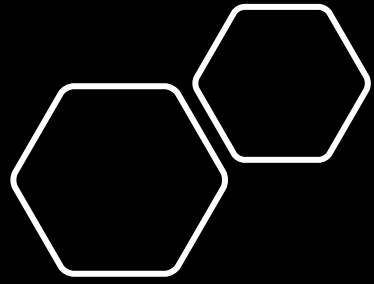
Data is the new oil





Whatever  
business you  
run...

---



.. it won't run  
without data

- Business data
- Management data
- HR data
- Technical data
- Network data
- Personal data (PII)
- Communications
- Mail data
- Financial data
- Operational data
- Intelligence
- Intellectual Property (IP)
- Ideas
- ...

**Other businesses want your data as well**







# Massive growth of digital business

- Direct marketing
- Data brokers
- Data Intelligence
- Data analytics
- Big data
- Artificial intelligence
- Machine learning
- Health care, research & development
- ...




A person wearing a grey hoodie is shown from the chest up, facing forward. The background is a dark field filled with glowing green binary code (0s and 1s) that appears to be floating or falling, creating a digital rain effect. The text 'But also ... the dark side' is overlaid in the upper left, and 'wants your DATA' is overlaid in the lower right.

But also ... the dark side

wants your  
**DATA**



# Your data in the wrong hands



EXPLOSIVES  
GRADE  
SIZE 1 1/4 X 8  
STUMPING  
50 lbs.



# Current state of crime

- Phishing
- Ransomware
  - not only encryption
  - data leak extortion
- Reconnaissance & Hacking
- Data breaches
- Biometric data
- Digital & Economical war



**Now the question is...**

**How  
do  
YOU  
get  
in control?**



**You can't simply lock it up...**







**because**

**data  
needs to flow**

**Data management essentials to get grip**



# How much €\$ can you spend to protect your data?





You can  
only protect  
what  
you know  
you have



Without  
an owner  
there is  
no protection



Nothing is

**stable**

Everything has

**a lifecycle**



Create

Dispose

Archive

Store

Update & Change





The start  
of the cycle is mostly  
short,  
easy to manage  
low security risk.



The end  
of the cycle is mostly  
long,  
difficult to manage  
high security risk.



Eeh...

What is risk?



Assets

Vulnerabilities (weaknesses/properties)

that can be exploited by

Threats (activities)

impact (\$\$ cost)



A background image of a balance scale, symbolizing balance and justice. The scale is a classic beam balance with two pans. On the right pan, there is a large, light-colored seashell. The scale is set against a light blue background. The text is overlaid on the scale.

**You need to balance**  
**the protection**  
**against**  
**the impact**



You don't want to

over-spend

or

under-protect



Your boss (or insurance)  
needs a budget  
Spreading cost

Your boss (or insurance)  
needs a budget  
Spreading cost  
over a year

Or 2..3..4..5.



# How to get started

# Getting grip on your data

Know the **external** context

- International regulations (GDPR, ...)
- National regulations (SOC, ...)
- Sector regulations (PCI-DSS, ..)
- Contractual obligations
- Enterprise vs PII/personal data requirements



# Getting grip on your data

Know the **internal** context

- Know your business (what)
- Know your organization (organigram)
- Make an inventory of processes and interfaces
- Assign business ownership
  - For each process
  - For each asset

# Getting grip on your data

Know the **processes**

- Know the data flow
- Know your sources (IN)
- Know the data processing
- Know your receivers (OUT)



# Getting grip on your data

Know the **data** in the processes

- Categorize your data - data types
  - Enterprise data
  - PII / Personal data (GDPR !)
  - Other ?

# Getting grip on your data

## Categorization (define data classes)

- Sensitivity = linked to business impact
- Ask the owner : "What if data is ..."
  - unavailable
  - changed
  - destroyed
  - leaked
  - accessed unauthorized, illegally, unlaw



# Getting grip on your data

## Categorization (define data classes)

- Categorize your data sensitivity
    - Enterprise data, for example
      - Unclassified, Official, Restricted, Confidential, Secret, Top Secret (NATO)
      - Public, Company internal, Confidential, Strictly confidential
- TLP RED TLP Amber TLP Green TLP White (public)

# Getting grip on your data

## Classification (apply the labels)

- Responsibility of owner
- Label all data
- Label containers if you can't label the data
  - Folder or File share
  - Data base
  - mailbox
  - ...



# Getting grip on your data

Mind the **lifecycle**

- Get started
- Keep going
- Start over again
- Think about security when
  - creating new processes
  - changing processes
  - removing processes
  - recheck on a regular schedule (even when nothing changes)

# Getting grip on your data

Mind the **business** and **legal requirement**

- Accountability & Responsibility
- Reporting & audit requirements (SOC I-II, ...)
- Incident management requirements
- Data breach requirements (GDPR)
- Subject rights



# Getting grip on your data

Mind the **business** and **legal requirement**

Reporting	SSAE-16					
	SAS70	SOC 1	SOC 2	SOC 3	Type I	Type II
Financail Standards		✓				
Security			✓			
Availability			✓			
Integrity			✓			
Confidentiality			✓			
Privacy			✓			
Public Report				✓		
System Design					✓	✓
Test System Design						✓
Retired	✓					

<https://www.icfiles.net/security/what-is-soc-2/>

# Consequences of data management **failure**

- Financial loss
- Business loss
- Reputation loss
- Contract SLA violation
- Regulatory violations
- Fines
- Prosecution
- Personal accountability



# Consequences of data management **failure**

Think about

- Direct and indirect impact
- Short term and long term impact
- How long can you survive a total breakdown?

**TAKEAWAYS**

# KISS (Keep it simple and stuff..)

- Manage enterprise data like personal data
- Keep the categories simple (<7)
  - 3 TLP (Red-Amber-Green) + 2 categories (public + highly critical)
- Define and maintain ownership
- Involve everyone
- Evangelize internal & external stakeholders (incl. customers...)
- Lead by example



# Use business best practices

- Use standards and frameworks
- ISO (international)
- NIST (US)
- ENISA (EU)
- COBIT (ISACA)
- ...

# Classification and labeling

- Force labeling
- Aim to classify everything
- Start with new data first
- Update labels when you change documents
- Set a **default label** for archived data that doesn't change
- Don't set public as default

# Think about the support processes

- Incident management (ISO 27035 & NIST)
- Data breach management (GDPR & other ...)
- Business continuity (ISO22301)
- Disaster recovery



**HOW HEXNODE  
HELPS  
COMPANIES  
ACHIEVE  
DATA COMPLIANCE**

**" From desktops to mobile devices to IoT,  
the device ecosystem  
is vast and heterogeneous. "**

Staying compliant with regulatory guidelines may be difficult, especially if  
devices are not within the confines of the organization.

# Here's how **Hexnode** can help

- Manage applications and ensure application security
- Ensure network and device security
- Enforce data security and compliance



**RISK:**

# UNAUTHORIZED ACCESS TO UNATTENDED DEVICES

**How  
Hexnode  
can  
HELP**

- Enforce strong password policies on devices.
- Enable data encryption on managed devices.
- Containerize and secure corporate data on personal devices.
- Track device location and lock down devices when outside work zones.

**RISK:**

# DATA ACCESS THROUGH UNSECURE APPLICATIONS

**How  
Hexnode  
can  
HELP**

- Uninstall or blacklist unsecure applications.
- Set up application permissions and configurations.
- Monitor and control per-app data usage.
- Disable file sharing options on managed devices.
- Disable copy/paste options to control data flow.
- Secure data by locking devices down in kiosk mode.

**RISK:**

# DEVICES DO NOT MEET SECURITY REQUIREMENTS

**How  
Hexnode  
can  
HELP**

- Patch any known vulnerabilities by updating device software and OS.
- Enforce restrictions and security configurations on managed devices.
- Prevent users from tampering with sensitive device features like USB debugging, factory reset, etc.



**RISK:**

# CHANCE OF COMPROMISE WHILE DATA IS IN-TRANSIT

**How  
Hexnode  
can  
HELP**

- Configure email and contacts and calendars
- Push Wi-Fi and VPN configurations and prevent devices from connecting to unsecured networks.
- Push web content filtering policies to keep corporate data safe from fraudulent websites.

**RISK:**

# UNMANAGED ACCESS TO SENSITIVE INFORMATION

**How  
Hexnode  
can  
HELP**

- Streamline access management using integrations with directory services (Azure AD, Okta, G-Suite).
- Deploy certificates to manage user access to corporate tools and services.
- Configure user and device groups on Hexnode to deploy resources based on roles and privileges.

**RISK:**

# **LACK OF VISIBILITY ON POLICIES AND OPERATIONS**

**How  
Hexnode  
can  
HELP**

- Monitor the security and compliant state of managed devices.
- Identify non-compliant devices and perform corrective actions on them.
- Remotely enable lost mode to protect corporate data on stolen or lost devices.
- Generate reports on device status and health.



**" Hexnode makes it **easier** for organizations  
to **maintain compliance** with  
regulatory requirements "**



July  
1.7

Questions



Q n A