

WELCOME AT THE

---

**BECHTLE**  
**SOLUTIONS SUMMIT**

# THE NIS 2 DIRECTIVE

Prepare your organisation for this regulation

---

**BECHTLE**



Nicolas Jans

Market Development Manager Security // Bechtle



Stijn Van Hoof

Business Development Manager // Exclusive Networks

# WHAT WAS NIS 0G AGAIN?

The predecessor of NIS 2

---



EU directive in 2016  
BE legislation 2019



Seven key-sectors



A minimum of security measures  
(risk management)



Identify operators of essential services



Increased EU cooperation



Report significant incidents

# OVERVIEW OF NIS 2

---



EU directive in 2022  
BE legislation TBD



More sectors and  
entities



New security  
measures  
(risk  
management)



New selection



Ownership



Report  
incidents V2

# BEFORE NIS

---



Healthcare



Transport



Energy



Water supply



Digital service providers



Banking and financial



Digital infrastructure

# AFTER NIS 2

Expanded scope to include more sectors and services as either essential or important entities



Providers of public electronic communications networks or services



Digital services such as social networking services platforms and data centre services



Waste water and waste management



Space



Manufacturing of certain critical products (such as pharmaceuticals, medical devices and chemicals)



Postal and courier services



Food



Public administration

# IMPACT

---



Passive selection



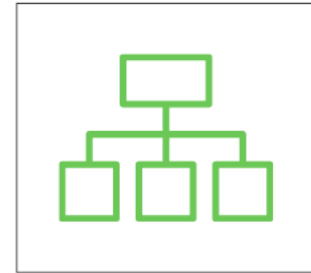
Management responsibility



Risk management & security measures



Incident reporting



Supervision & sanctioning

# PASSIVE SELECTION

---



(sub) Sector



# employees



Revenue



3 categories



# MANAGEMENT RESPONSIBILITIES

---



Approve risk  
management  
measures



Oversee  
cybersecurity  
measures  
implementation



Liabile non  
compliance



Offer proper training



Follow training

---

CYBERSECURITY



**Former Uber CISO Faces  
Prison Time For  
Mishandling Cyberattack:  
Justice, Scapegoating, or  
Both?**



# RISK MANAGEMENT

---



Annual supply chain  
risk assessment



Roles,  
responsibilities,  
authorities



Risks documented  
& approved



Threat  
intelligence



Asset vulnerabilities  
identified  
documented

# SECURITY MEASURES

---



Awareness and  
training



Technical security  
measure



Governance



Muti-standard  
frameworks (NIST,  
CIS, ISO21XXX)



Proportional  
requirements and  
assurance

# INCIDENT REPORTING

---

Essential and important entities notify, without undue delay any incident that has a significant impact on the provision of their services.

24h

- Early warning (telephone, mail) + whether it is presumed malicious, or cross border
- (Full notification for trust service providers)



72h

Official incident notification: assessment of the incident, severity and impact + indicators of compromise



1 month

- Final report
- Intermediary reports at request CSIRT
- Final report 1 month after end

# SUPERVISION

Before or after incident

After incident

	Essential	Important
On & offsite inspections	✓	✓
Targeted security audits	✓	✓
Security scans	✓	✓
Request information	✓	✓
Regular audits	✓	✓
Evidence policies	✓	✓
Fine	10 M or 2% AR	7M or 1.4% AR

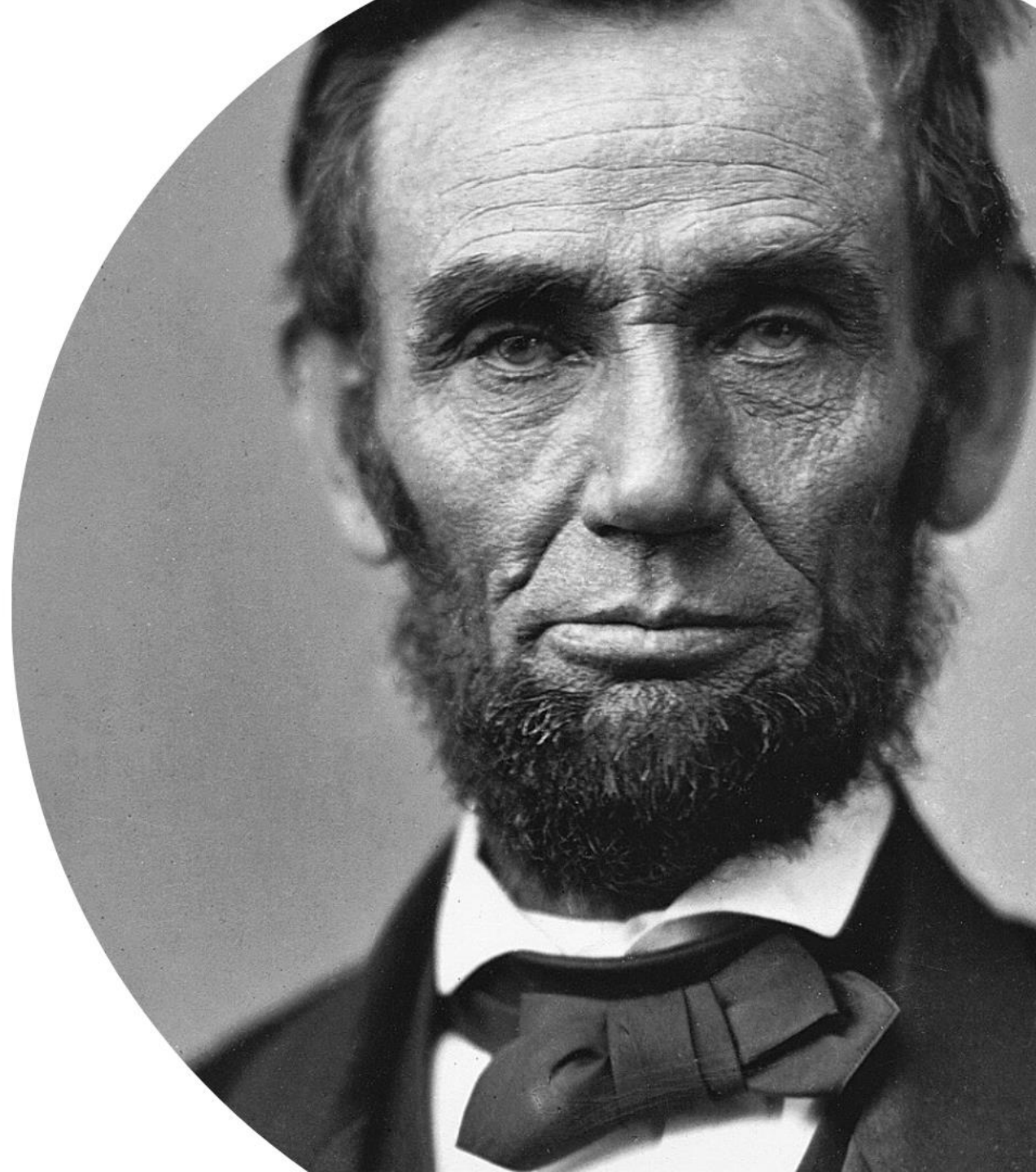
# BUY NOW AND BE COMPLIANT

”

---

Don't believe everything you read on the internet just because there's a picture with a quote next to it.

Abraham Lincoln



# COMPLETE SECURITY

---

**BECHTLE**

Network	Endpoint	Cloud
NGFW	EPP	MFA
SIEM	EDR	SASE
ZTNA	XDR	IAM
PENTEST		



# SECURITY AWARENESS

---

- Risk score
- Automatic simulations
- Behavioral change



# WANT TO TALK SECURITY?

---

SEE YOU AT THE PHISHING TANK