



**Hewlett Packard  
Enterprise**

# **DIGITAL RESILIENCE AND DORA**

Graham Rogers  
Solution Architect  
NED EMEA and LATAM

11<sup>th</sup> April 2024

# THE IMPORTANT QUESTION

---

**How do you know you have had a cyber attack?**



# WHY DIGITAL RESILIENCE MATTERS

- Phishing remains an epidemic
- Ransomware attacks are getting simpler than ever – and the threat is changing
- Hostile nation states are on the rise
- Insider attacks are increasing and changing
- Vulnerabilities hit a record high

## \$4.4M RANSOM

“Colonial Pipeline confirms it paid \$4.4m ransom to hacker gang after attack”

## SOLARWINDS USED IN HACK

“How Russia used SolarWinds to hack Microsoft, Intel, Pentagon, other networks”

## CATASTROPHIC

“Cyber-attack on Irish health service ‘catastrophic’ ”



## \$200K PAYOUT

“US water filter supplier pays \$200K to settle credit leak lawsuit”

## HIT BY RANSOMWARE

“US meat supply hit by suspected Russian ransomware attack on JBS, world’s top meat processor”

## DISRUPTED OPERATIONS

“Packaging vendor Ardagh admits cyber-attack disrupted operations”

## WHY RESILIENCE MATTERS?

### US Flight Grounded due to system failure

The overnight outage affected the Notice to Air Mission Systems (NOTAM), a crucial notice to pilots for flying information.



The NOTAM database file corruption caused the 7-hour outage with cascading impact on air traffic.

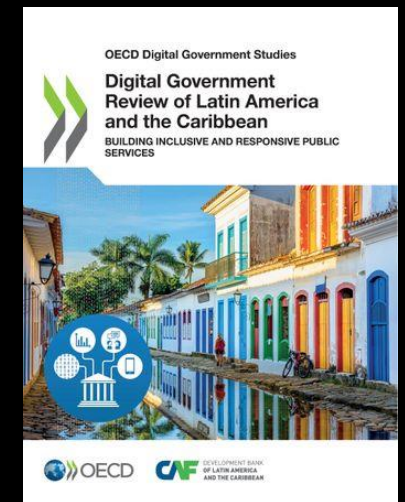
- 11000 flights impacted
- Corrupted database file
- Both primary & backup impacted
- Human error, Procedure not followed
- System upgrade planned in 2028-29

Source - <https://arstechnica.com/information-technology/2021/10/facebook-outage-likely-caused-60m-loss-impacted-small-businesses/>

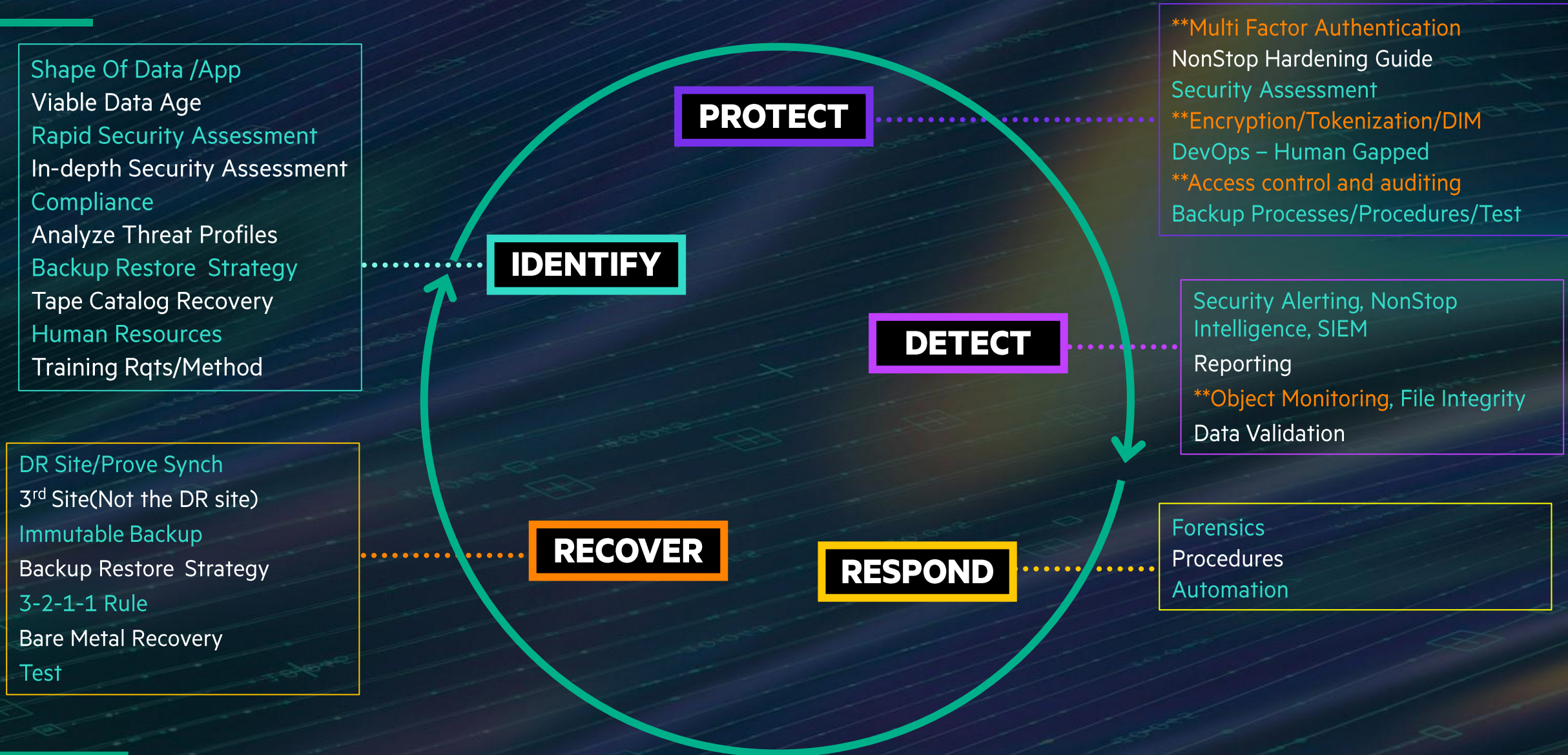
# INCREASING REGULATION – AROUND DIGITAL RESILIENCE

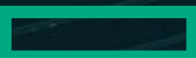
## Good Practice now being Mandated

- Digital Operational Resilience Act - EU
- Financial Services Conduct Authority, UK
- Saudi Monetary Authority
- FBI
- Investigating Latin America...
  - OECD (Organisation for Economic Co-operation and Development)



# DIGITAL RESILIENCE – THE ENDLESS LOOP



 Aligned with NIST Cybersecurity Framework

# **DORA – NED INFRASTRUCTURE OPINION ONLY**

---

All Information sourced from the “DORA FINAL TEXT” section

- [https://www.digital-operational-resilience-act.com/DORA\\_Articles.html](https://www.digital-operational-resilience-act.com/DORA_Articles.html)

All the information gathered is my research/opinion and is NonStop Infrastructure focused

It is essential that you work with your own organisation to define what you have to do and how DORA affects you



# DORA – EU – DORA COMPLIANCE EXPECTED 2025

- Legislative weight of DORA – Administrative & (potential) Criminal penalties
- DORA is a Regulation, not a Directive, so it is binding in its entirety and directly applicable in all EU Member States.

- **The Board is**
- **Accountable!!!!**

DORA PILLARS	KEY REQUIREMENTS
ICT Risk Management	<ul style="list-style-type: none"> <li>• <b>Business continuity and Disaster Recovery plans – a must</b></li> <li>• A set of key principles revolving around specific functions – identification, protection and prevention, detection, response and recovery, learning and evolving and communication</li> <li>• Most of them are recognized by current technical standards and industry best practices, such as the NIST framework</li> </ul>
ICT Incident Reporting	<ul style="list-style-type: none"> <li>• <b>Cybersecurity and reporting processes – a requirement</b></li> <li>• Implementation of an ICT-related incident management process</li> <li>• Classification of ICT-related incidents</li> <li>• Reporting of major ICT-related incidents</li> </ul>
Digital Operational Resilience Testing	<ul style="list-style-type: none"> <li>• <b>Annually tested – including remediation plans</b></li> <li>• Basic Testing of ICT tools and systems – Applicable to all financial entities</li> <li>• Advanced Testing of ICT tools, systems and processes – Only applicable to financial entities identified as significant by competent authorities</li> </ul>
ICT Third-Party Risk Management	<ul style="list-style-type: none"> <li>• <b>ICT third-parties are subjected to EU oversight</b></li> <li>• DORA introduces requirements on both financial organizations and critical technology providers</li> <li>• Financial organizations are required to compile a standard register of third-party technology providers, the service they provide and the critical functions they underpin</li> <li>• New criteria for risk assessment of 3rd party technology service providers</li> </ul>
Information and Intelligence Sharing	<ul style="list-style-type: none"> <li>• <b>Encouraged to share threat information and intelligence</b></li> <li>• DORA introduces guidelines on setting up information sharing arrangements between firms to exchange among themselves cyber threat information and intelligence on tactics, techniques, procedures, alerts and configuration tools in a trusted environment</li> </ul>

# **DORA STRUCTURE – “DORA FINAL TEXT”**

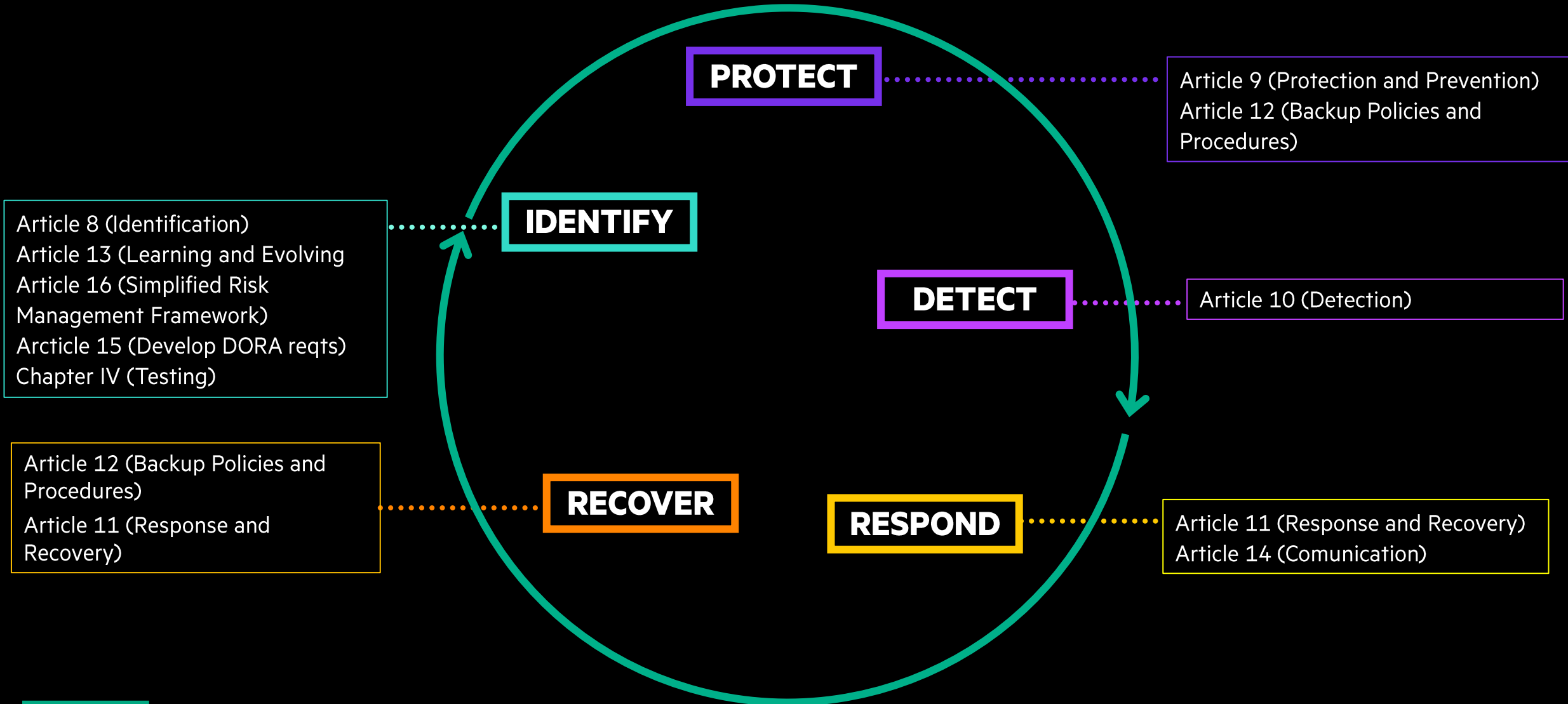
---

All Information sourced from the “DORA FINAL TEXT” section

- [https://www.digital-operational-resilience-act.com/DORA\\_Articles.html](https://www.digital-operational-resilience-act.com/DORA_Articles.html)
- Chapter I – General Provisions – Article 3 - This is a must read particularly useful is Article 3 “Definitions”
- Chapter II – ICT Risk Management – The focus of this presentation NonStop Infrastructure
- Chapter III – ICT Related Incident Management Framework
- Chapter IV - Digital Operational Resilience Testing
- Chapter V - Management OF ICT Third Party Risk
- Chapter VI - Information Sharing Agreements
- Chapter VII – Competent Authorities
- Chapter VIII – Delegated Acts
- Chapter IX – Transitional And Final Provisions



# DIGITAL RESILIENCY – DORA CHAPTER II RISK MANAGEMENT



## **FUTURE – EVOLUTION – PART OF THE IDENTIFY ENDLESS LOOP**

---

- Current RVU L23.08 has \$SYSTEM BM Recovery - DONE
- vNS – Spacesaver Spare Wheel – gives us options (VIO...)
- Your process review and evolution
- Ongoing HPE NonStop and Partner improvements and new functionality to improve DR support and implementation
- Continuous analysis of evolving attack profiles, working with partners and customers
- Quantum Safe Cryptography
  - PQC – Post Quantum Cryptography
  - New NIST requirements – harvest now decrypt later



**THANK YOU!**

