LAWRENCE
DATA PROTECTION · AI · TECH

HUNT & HACKETT

# Is your incident response process ready for today's EU notification landscape?

A SIX-STEP SELF-ASSESSMENT

**Step 1 → The incident: what has been observed?**
*Can your security team establish a reliable initial picture within the first few hours?*

- ☐ We can quickly determine which systems have been affected and in what sequence.
- ☐ Our logging and telemetry provide sufficient information to reconstruct an initial timeline of the attack.
- ☐ We know which systems fall outside our monitoring scope.
- ☐ We can distinguish the type of incident at an early stage—such as ransomware, data theft, Business Email Compromise (BEC) or cyber espionage—because the response differs for each.
- ☐ From the outset, we document what has been confirmed, what is considered likely and what remains unknown.
- ☐ Within 24 hours, we can identify which internal and external stakeholders need to be involved in decision-making.

**Step 2 → Applicable regulatory frameworks: which legislation may apply?**
*Does your legal or compliance team assess the relevant regulatory frameworks before a notification decision is made?*

- ☐ We know which EU regulatory frameworks apply to our organisation: GDPR, NIS2, DORA, the Cyber Resilience Act (CRA) and/or the AI Act.
- ☐ For every incident, we carry out a brief assessment across three areas: data, service delivery and technology.
- ☐ We know which regulator is responsible under each regulatory framework.
- ☐ We understand that a single incident may have multiple legal implications and respond accordingly.
- ☐ We have mapped which systems, business processes and categories of data fall within the scope of each regulatory framework.

**Step 3 → Forensic findings: what actually happened?**
*Does your forensic investigation produce findings that can be interpreted from a legal perspective?*

- ☐ We have immediate access to forensic expertise whenever an incident occurs.
- ☐ During a live incident, we can prioritise forensic activities without compromising containment or recovery.
- ☐ We can carry out an initial root cause analysis while containment activities are still underway.
- ☐ For every finding, we explicitly distinguish between what is confirmed, what is considered likely and what remains unknown.
- ☐ We can establish when the initial compromise occurred, independently of when the incident was detected.

**Step 4 → Legal assessment: which notification obligations are triggered?**
*Can your legal team make a robust legal assessment based on the forensic findings?*

- ☐ Our legal and forensic teams work from a shared incident vocabulary.
- ☐ We make evidence-based provisional assessments rather than waiting for complete certainty.
- ☐ We understand the different notification deadlines under each regulatory framework and know when those deadlines begin.
- ☐ Legal triggers are translated into specific forensic questions, and forensic findings inform the legal assessment.
- ☐ We have clearly defined decision points for the first 4, 24 and 72 hours.

**Step 5 → Notification(s): to the right authority, in the right format, within the right timeframe**
*Is your notification process designed to support multiple parallel reporting obligations?*

- ☐ We have defined in advance who is authorised to make notification decisions.
- ☐ We understand the distinction between an early warning, an incident notification and a final report.
- ☐ We can submit a technically substantiated notification while the forensic investigation is still ongoing.
- ☐ We have escalation procedures that activate both forensic and legal expertise from the very first hour.
- ☐ We have previously practised preparing notifications under time pressure.
- ☐ We actively manage the schedule for follow-up notifications and interim reports.

**Step 6 → Evidence file: can your decision-making be reconstructed afterwards?**
*Are you building the evidence file during the incident so that your decisions can later be justified?*

- ☐ We build the evidence file throughout the incident, not afterwards.
- ☐ For every decision point, our records clearly show what we knew at the time, what we did not know and why.
- ☐ We can explain why a notification was or was not made at a particular point in time.
- ☐ Forensic findings and legal assessments are maintained within the same evidence file.
- ☐ Regulatory reporting and legal review are treated as ongoing activities rather than the final stage of incident response.

**What does your score tell you?**
This checklist is not a pass-or-fail assessment. Instead, it highlights where your incident response process is robust and where it is likely to come under pressure when time is critical.

**Mostly missing ticks in steps 1, 3 or 6?**
Your technical foundations may require attention. Consider your logging, data retention, forensic capability and the quality of your initial fact-finding. These are the building blocks that determine how well your organisation can justify its decisions when questioned by a regulator.

**Mostly missing ticks in steps 2, 4 or 5?**
Your legal preparedness may need strengthening. Consider your regulatory framework mapping, notification thresholds and whether your escalation procedures bring the right expertise into the process quickly enough.

**Missing ticks across multiple steps?**
This usually indicates that your technical and legal teams are not aligned—making it much harder to respond effectively under pressure. Would you like to find out whether your assessment reflects reality?

Hunt & Hackett and Lawrence Advocaten would be pleased to help you evaluate your incident response capability.

Lawrence is an innovative law firm specialising in Data (Protection), AI & Tech. We believe that legal expertise must continuously evolve to keep pace with the world of tomorrow. That's why we combine in-depth knowledge with creativity and technology to help clients seize opportunities and manage risks.

🔗 www.lawrence-advocaten.nl
www.linkedin.com/company/lawrence-advocaten/
+31 6 2079 1755

Hunt & Hackett is a cybersecurity company that protects European businesses against digital threats and espionage. We operate as a managed detection & response (MDR) and incident response partner, with specialists who work on the front line of cyber conflicts every day, helping organisations prevent, detect and respond to cyberattacks.

🔗 www.huntandhackett.com
www.linkedin.com/company/huntandhackett
+31 70 222 0000