Cyber Crisis Damage Control Checklist.

Most organisations focus on prevention primarily. But reality is that although the highest walls and deepest moats will reduce risks, they will not be able to keep out every intruder all the time. So, here is the follow up question: what's your playbook after a cyber-attack?

How fast can you detect and isolate?
How do you get your operations up and running again?
And are you ready to communicate adequately and timely?
In short: how do you minimise the damage?

This checklist will help you to identify which steps you have already taken and where you can still take action.

---

1. **Detection:** See Faster, Act Faster

- ◯ Monitoring for suspicious activities; backups checked for malware.
- ◯ Network segmented and designed with security principles.
- ◯ Detection tools (NDR/XDR/SIEM) properly configured.
- ◯ Alerts linked to 24/7 on-call and clear escalation procedures.

---

2. **Isolation:** Contain the Damage

- ◯ Freeze systems and isolate affected areas quickly.
- ◯ *Isolated Recovery Environment (IRE)* in place, tested
- ◯ *Privileged Access Management (PAM)* active, enforced.
- ◯ Identity recovery processes prepared.

---

3. **Recovery:** Returning to Business Faster

- ◯ Backups regularly tested for restorability, including immutable backups.
- ◯ Recovery plans are automated, documented, and aligned with business priorities.
- ◯ Forensic and recovery partners are pre-selected and tested.

---

4. **Continuity:** Keeping the Business Running

- ◯ Critical processes and dependencies identified and documented.
- ◯ Cyber recovery integrated with Business Continuity Plan (BCP).
- ◯ Operational continuity regularly tested with external partners.
- ◯ SOC and forensic partners pre-engaged for support.

---

5. **Communication:** Order in the Chaos

- ◯ Cyber incident communication plan tested and aligned with PR/compliance.
- ◯ Contact lists up to date; alternative channels tested.
- ◯ Stakeholder notifications pre-drafted and ready.
- ◯ Human factors (stress, burnout) considered.

---

6. **Data & Privacy Compliance:**
Meeting Regulatory Requirements

- ◯ Applicable laws, regulations (GDPR, DORA, NIS2, sector-specific), and supplier agreements are understood.
- ◯ Incidents promptly reported to authorities
- ◯ Data management (register, storage location, conditions) are up to date.
- ◯ Privacy by design applied in all new projects and systems.

Next Steps
Do you want deeper insight into where your organization may still be vulnerable?
Please take the **Cyber Quick Scan** and receive an instant overview per focus area. This will point out your strengths, and show which areas need attention.

Plan a call.
How Yuma can make your organisation more resilient?

Christiaan Driessen
+31 6 83 12 08 88

yuma