



Crisis in practice

The golden hour of a cyber crisis, and the six steps that decide it

CyberBusters B.V. · practice paper · version 1.0

In the first hours a crisis rarely fails on technology, and not on composure either.

It fails on authority, and then on follow-through. The room is full of people who know what should happen, and nobody is sure they are allowed to have it done. What is decided after that is often said into the room rather than handed to someone.

This paper describes that chain, and how to put a clock on it.

Summary

Behaviour under pressure has been thought about well. There is a well-founded model of crisis skills, resting on research from firefighting, aviation and disaster medicine. That model describes how people hold up when things get tense, and it describes it well.

This paper is about something else, a layer underneath. Not how the team behaves, but what happens to the decision: who took it, who carried it out, and whether anyone checked. That is not a property of people but of the chain between them, and unlike behaviour, that chain can be timed.

Six steps make up that chain: picture, judgement, decision, order, check, handover. The first five come from Dutch crisis management practice, known as BOBOC. The sixth appears in no model and happens in every long crisis.

1. A Wednesday afternoon in October

On Wednesday 21 October 2026 two critical vulnerabilities in PHP became public, ahead of the planned disclosure and with working proof of concept code alongside. The Dutch NCSC wrote that morning that they can be exploited with a simple POST request, and at 11:03 reported it had not observed active exploitation. There were no patches yet at that point.

What happened next is better documented than most crises, because two organisations wrote their decisions down with the time attached.

The NCSC took its own website offline as a precaution. The hosting provider Mijndomein decided at 13:35 that all customer websites would go offline preventively until the update arrived; by 14:30 it was done. They published the reasoning: temporary unavailability is a smaller risk for us than the possibility of a break-in. Over the evening they rolled out the new PHP versions, and only the next morning at 11:20 did it say resolved.

Read that sequence again with the six steps of this paper beside it. **Picture:** are we running a vulnerable version, and where. **Judgement:** unavailability against the chance of a break-in. **Decision:** at 13:35, by someone allowed to take it. **Order:** by 14:30 it was done. **Check:** the update applied, the sites back. **Handover:** it ran through the night and was only finished the next morning.

This is not an exceptional crisis. It is here because it happens to have been written down, and because every step described further on can be found in it with a timestamp.

2. Where the first hours go

In trauma care the first hour is called the golden hour. Whether those sixty minutes are exactly right is contested in the literature, and that is not the point here. The point is why it works: nothing brilliant happens in that hour. A sequence is fixed, everyone knows their role, and nobody has to ask whether they are allowed.

A cyber crisis has such an hour too, and there the sequence is usually not fixed.

Ask after a real crisis where the time went, and the answer is seldom about technology. It is about the stretch in which everyone knew what ought to happen and nobody set it in motion.

That stretch has a cause that is easy to name and hard to fix: it is unclear who may do what. On paper it is often written down. In the room the question is whether this is the case that rule covers, whether the situation is bad enough, and whether the person who may decide can be reached.

The result is a decision that comes too late, or one that comes without anyone carrying it. The second is worse, because then nothing happens while everyone believes it has been handled.

3. Behaviour is half of it, structure the other half

A team that stays calm, keeps an overview and can improvise starts from a better position. That is obvious and it is well researched. We do not replace that and we do not claim that ground.

But composure without authority produces nothing. A team can establish, in perfect calm, that the production line has to come down, and then wait forty minutes for someone to call back. The problem was not the behaviour.

So we look at the chain: from the first alert to a measure that was demonstrably carried out. Not because behaviour does not matter, but because the chain is the part you can record and measure again next year.

That is what the golden hour does in trauma care as well. What is fixed there is not the clinician's composure but the sequence around them. Structure makes behaviour matter less, and that is exactly what you want on a night when nobody is at their best.

4. The six steps

Six steps. Five of them are BOBOC, the Dutch crisis management sequence: forming a picture, forming a judgement, taking a decision, issuing an order, and checking. The last two are missing from models about behaviour, and they are exactly where a decision evaporates.

The sixth step is the handover. It appears in no model and occurs in every crisis that lasts longer than a shift.

	Step	What goes wrong	What you measure
B	Picture	What happened? Four group chats and a phone list are not a picture. Without agreed moments the picture drifts per person, and then two people negotiate about a fact instead of about a decision.	How long until there is one picture, and in how many places it lives.
O	Judgement	What does it mean? Speed against care, containment against keeping production running, openness against legal caution. Leave that weighing unspoken and you still make it, only nobody can retell it afterwards.	Which trade-offs were made explicitly, and which only implicitly.
B	Decision	What are we going to do about it? This is where the twenty to forty minutes go. The room is full of people who know what should happen, and nobody is sure they are allowed to have it done.	Time to the first decision that has an owner.
O	Order	Who is going to do it? A decision that does not become an order is an opinion. In aviation and in the operating theatre an order is repeated back before it is carried out; in a crisis room it is usually said into the room.	How many decisions became orders, and how many were left hanging.
C	Check	Has it been done? Looking back does not start afterwards. An order that was never checked is an assumption on which the next three decisions rest.	How many orders were checked before the picture moved on.
+	Handover	Who takes it over? No model covers this, and it happens in every long crisis. At midnight the shift changes and whatever was not written down disappears: the assumptions, the open orders, and the reason something was rejected earlier.	What is lost at the change, and how long recovery takes.

5. In OT, stopping is a different decision

In an office environment the heavy decision is usually whether to restore now or preserve evidence first. In an industrial environment another decision arrives that is of a different order: whether the installation may keep running.

That decision is not a security decision. It touches safety, it touches delivery, and it sits with someone other than the CISO. In practice that is why it stalls: the security side does not dare take it and the production side does not know it is theirs.

On top of that, the information the decision rests on is itself suspect. If process data can no longer be trusted, you do not know whether the installation is doing what the screen says. Forming a picture is therefore not a collecting step in OT but a judgement in its own right.

The trail is the same; the content of each step is not. That is why we rehearse OT and IT separately rather than running the same scenario in different clothes.

6. What you measure, and what a score is not

Each of the six steps has one observation with a clock or a yes or no attached. Not a facilitator's impression, but a time or a count. That makes it retellable and, more importantly, repeatable: the same six measurements in a later exercise show whether anything changed.

Never next to a name. The outcome is about the chain, not about a person. A time that ran long says something about the agreement that was missing, and rarely about the person who stood waiting.

And a good result is no guarantee. An exercise is an exercise: the consequences are not real, the day was chosen and everyone knows they are taking part. What you measure is whether the chain works in conditions that resemble it, not whether it holds in conditions that are it.

7. What the law asks of this

The Dutch Cyberbeveiligingswet places a number of things with the board. The measures require its approval (article 24(1)), and every board member has the knowledge and skills to identify risks, assess measures and weigh their consequences for the entity's own services (article 24(2)). That must be met within two years of that provision entering into force (24(3)), kept demonstrably current (24(4)), and evidenced by a certificate showing participation in a training covering those subjects (24(5)).

Note the word participation. The law asks for no examination, no accreditation and no recognised scheme. Rules on the duration and level of such a training may still be set by secondary legislation (24(6)); at the time of writing they do not exist.

When the clock starts is not in the law. Article 107 leaves entry into force to a royal decree that may differ per article or per part. Anyone claiming the period started on a particular date is claiming more than the text supports.

Separately, a significant incident starts a twenty-four hour clock for the early warning, and it starts on becoming aware, not on understanding. That is a decision under uncertainty, and it falls precisely in the third step of this trail.

8. Limits of this paper

This is a practice paper. The trail comes from what we see in crisis rooms and from existing working methods, not from our own research. We have not shown that a short time to the first decision correlates with a better outcome in a real crisis; that would require observation during real crises, and those are not arranged for research.

The six steps are also not cleanly separable. Picture and judgement run into each other, and checking produces a new picture. The trail is a way of looking, not a law of nature.

And it is half the story. The other half is about behaviour under pressure, and better papers than this one have been written about that.

9. Closing

A plan describes who takes which decision. An exercise shows whether that decision is actually taken, by whom, and what happens to it afterwards.

The difference between those two is why rehearsing cannot be replaced by reading. Not because people fail to understand it, but because a chain only becomes visible once something has to pass through it.

Sources

This paper rests on the following practices and texts. The list is short on purpose: what lies underneath, and no more than that.

- Cyberbeveiligingswet (the Dutch NIS2 implementation), in particular articles 21, 24, 26 and 107. Statute via wetten.overheid.nl.
- Directive (EU) 2022/2555 (NIS2), via EUR-Lex.
- BOBOC, the Dutch crisis management sequence for forming a picture and a judgement, taking a decision, issuing an order and checking.
- Klein, G. A. (1993). A recognition-primed decision model of rapid decision making. On deciding with incomplete information.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. On forming a picture as more than perceiving.
- Weick, K. E. (1993). The collapse of sensemaking in organizations: the Mann Gulch disaster. On what happens when the shared picture collapses.
- NCSC (NL), PHP vulnerabilities (CVE-2026-109618 and CVE-2026-109619), community.ncsc.nl/p/php, accessed 22 October 2026, and advisory NCSC-2026-0443.
- Mijndomein, status notice on the PHP vulnerabilities, 21 and 22 October 2026.
- Reading an order back and structured handover are practices from aviation and healthcare. This paper uses them as working methods and makes no claim about the research literature behind them.