Newsletter issue 3 - 14 May 2026

The First Hour: who is allowed to act?

Why the first hour becomes a governance problem long before it becomes a recovery exercise.

When ransomware becomes real

The previous newsletter issue focused on what remains controllable when a critical dependency becomes unsafe. This issue moves one layer closer to the organisation itself: when pressure is rising, what matters just as much is who is actually allowed to act before full certainty exists. The recent ChipSoft ransomware incident made that dependency question very concrete for healthcare leaders. When a trusted supplier route is restricted, systems are disconnected as a precaution, or patient-facing services are temporarily unavailable, the issue quickly moves beyond technology. It becomes a question of authority: who is allowed to decide what must be narrowed, paused, isolated, or kept running while the facts are still incomplete?

The Odido case adds another layer to that same question.

There, services remained available, but trust did not simply return because the network kept working. Customers had to check whether their details were part of the stolen dataset, remain alert to convincing phishing attempts, and deal with the uncertainty that personal data may continue to create risk long after the incident itself has moved out of the headlines.

That is why the first hour matters beyond the first hour.

When identity, access, customer data or dependency routes become uncertain, delayed containment does not only create technical exposure. It can create a longer trust problem for the people outside the organisation as well.

Victims rarely describe ransomware as a clean technical event. They describe **powerlessness**, **disruption**, and a **long personal aftershock**. In Dutch reporting, one victim said it ***"felt like a robbery"***, another described the **lingering shock months later**, and another spoke of **customers literally arriving at the door with clubs after operations had collapsed**.

In critical environments, the consequences can extend even further. In the UK, the Synnovis ransomware attack later became linked to a patient death after disruption to pathology services and delays in obtaining vital test results were identified as contributing factors. That matters not only because of the victim, but because every such incident also leaves a family, a care team, and a leadership team carrying consequences that cannot be undone.

That is the part many organisations still underestimate: the human cost often begins while the incident is still unfolding.

The first hour is not mainly technical

A live ransomware incident quickly stops feeling like a systems problem and starts becoming a governance burden.

Experienced leaders are forced to make high-impact decisions without full certainty. Teams lose sleep. Confidence begins to crack, and every unanswered

- One Lesson

If authority is not pre-agreed, the first hour is negotiated — not governed.

question adds weight. The fear is no longer only that the attack happened, but that the next decision may either contain the damage — or deepen it.

This is where powerlessness, guilt, second-guessing, and the longer aftershock often begin. Not after the incident, but in the middle of it — when responsibility is high, facts are incomplete, and control starts to feel fragile.

Not whether an alert fired.
Not whether the SOC saw something unusual.
Not whether a playbook exists somewhere.

But who is allowed to act while the facts are still incomplete.

- Who is allowed to isolate systems?
- Who is allowed to revoke access?
- Who is allowed to shut down services or force degraded operations?
- Who is allowed to override business owners if delay increases the blast radius?
- What level of uncertainty is enough to trigger action?
- Which actions are pre-agreed, and which still need permission?

That is the real middle of the incident.
And it is where many mature organisations still struggle.

Why organisations still lose the first hour

Most cyber discussions begin in the wrong place.

They begin with recovery, with restoration, with lessons learned afterward.

But for the people inside a live ransomware incident, the first hour is rarely defined by recovery.

It is defined by authority.

Who has the right to act?
Who can make the call?
Who can move before every fact is known?

That is where many organisations lose time they can no longer afford to lose.

Not because nobody noticed the incident.
But because action was not pre-agreed.

In many environments, awareness arrives before control does. The real test is whether a credible signal can trigger a safe move quickly enough to matter.

- Board Question

Have we pre-agreed who can make the first containment move before full certainty exists?

Why so many organisations are still not ready

Research commissioned by the UK Home Office found that many ransomware victims had little awareness of the risks and impacts before their attack, were unprepared for the scale and sophistication of what followed, and were often unclear on the key steps needed to mitigate ransomware. The same research also found that very few organisations described having a business continuity plan specific to cyber or ransomware.

That should concern leaders. Because where there is no clear, tested path, people are left carrying more than disruption: they carry uncertainty, pressure, second-guessing, and often guilt about the decisions made under incomplete trust.

A business continuity plan can reduce that burden — but only if it has been pressure-tested well enough to remain useful when the incident is live, the facts are incomplete, and authority has to translate into action.

A plan on paper is not the same as control under pressure.

Investment is not executable control

Many organisations have invested heavily in prevention, detection, monitoring, backup, and response readiness.

And still, mature environments should assume that a credible signal may one day arrive despite all of that — not because the organisation was careless, but because prevention lowers the chance of an incident; it does not remove the need for control in the first hour.

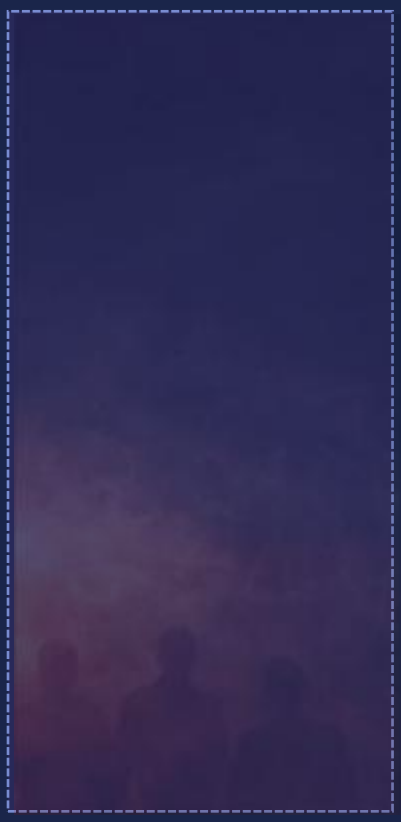
When a ransomware incident becomes live, the hardest questions are not theoretical.

They are immediate:
Who can pull the trigger?
Who can isolate?
Who can revoke?
Who can force degraded operations?
Who can make the difficult trade-off between continuity and containment before the damage spreads further?

This is why I keep coming back to a point that is easy to miss:

Detection is not the same as control.

Because control depends not only on seeing the problem, but on whether the organisation has already decided who is allowed to act when certainty is still incomplete.



- Pressure Point

Most organisations do not lose the first hour because nobody saw the problem. They lose it because the hard move is still waiting for permission.

Where the incident gets bigger

You can detect malicious activity and still lose critical time.

You can have good tooling and still hesitate.

You can have strong people and still face a situation in which the next move is obvious operationally, but unclear organisationally because no one is fully authorised to make it.

That is where the incident grows.

Not always because people made the wrong decision.
Often because the right decision was not pre-authorised strongly enough to be executed under pressure — and that is how hesitation turns into cascade.

The attacker does not wait for clearer governance. Delay is not neutral; it changes the shape of the incident.

And that matters, because the consequences are rarely limited to temporary inconvenience.

A 2024 Forrester study commissioned by VMware found that 99% of leaders whose organisations had faced a ransomware attack reported at least one serious consequence, and 77% reported three or more.

Those consequences included revenue loss, ransom payments, job losses, IP loss through exfiltration, board or C-suite accountability, and reputational damage.

In other words: the cost of delay is not theoretical either.

Speed is permissioned

The first hour is often described as a race against time.

That is true. But it is equally a test of governance.

Because speed is permissioned.

If authority is not pre-agreed, the incident is negotiated — not governed.

Security may want to isolate.
Operations may want to wait.
Business owners may fear unnecessary disruption.
Leadership may want one more confirmation before approving a hard move.

And while that negotiation continues, the attacker does not pause.

This is why I do not think the real resilience gap is only about prevention. It is about whether organisations have turned awareness into authorised action.

– Speed Is Permissioned

Delay is not neutral.

If the hard move still needs approval, the incident keeps moving while the organisation negotiates.

The missing operational layer

That is also where I believe many organisations need a different operational layer.

Not another awareness layer.
Not another abstract assurance exercise.
But a containment layer that helps leadership act decisively once the incident is already live.

Because authority on its own is not enough.
Authority still needs a safe move.

That is the gap I focus on.
Not replacing the existing stack.
Not dismissing the money already spent on EDR, SIEM, backup, and response.

But helping organisations turn decision rights into executable control when hesitation becomes expensive and the first safe move has to happen before full certainty arrives.
In practice, that means giving leadership a way to act without waiting for the whole picture to become clear.

A way to reduce exposure, interrupt malicious behaviour, narrow the blast radius, and preserve enough operational room to keep the incident governable. Not just knowing that action is needed — but having a move that is safe enough to authorise and practical enough to execute.

The goal is simple:
Stop the cascade before uncertainty, delay, and spread become much harder to contain.

Why this is also a human crisis

Recent academic work argues that ransomware should be understood as a whole-of-organisation crisis phenomenon rather than merely an IT issue, and explicitly documents severe organisational harms, including a quoted victim experience of **"a bit of PTSD"** every time they walked through the office door.

That human residue matters more than many board conversations admit.

The Odido aftermath shows how that residue can also sit outside the organisation.

When personal data has been exposed, affected people are not simply "notified". They are asked to stay alert, verify calls, monitor suspicious messages, check whether their details appear in leaked datasets, and live with the possibility that someone may use familiar information to make fraud feel credible.

– What Containment Changes

Authority only matters if the organisation also has a safe operational move available. Containment turns decision rights into executable control.

That is not a technical after-action item.

It is a trust burden transferred to customers, citizens, patients, employees or partners.

The UK Home Office research found that stress was the most common psychological impact among victim organisations, with respondents describing long-term effects including **sleep loss**, **appetite loss**, **anxiety**, and **guilt** among IT staff and senior leaders.

So, when we talk about the first hour, we are not only talking about timing.

We are also talking about the burden people are forced to carry when authority is unclear, decisions are delayed, and control slips further than it needed to.

The difference between a hard incident and a long, corrosive one is often shaped in that first period — not only by what is seen, but by what is allowed.

The real question for leadership

The practical question every CIO, CISO, and board should be able to answer before the next incident forces the issue is not only:

Do we have the right tools?
It is:
Who is allowed to act, on what trigger, and with what authority, before the damage becomes harder to contain?

Because if authority is still being negotiated while the incident is already moving, **speed becomes friction, and control becomes fragile**.

What can still be prevented

Much of the suffering that follows a ransomware attack can be prevented.

Not all uncertainty can be removed.
Not every consequence can be avoided.

But control does not have to collapse because authority was unclear, action was delayed, or the right move was still waiting for approval.

When decision rights are pre-agreed, triggers are clear, and containment can be executed safely, the first hour becomes more governable.

And when the first hour is more governable, a great deal of the chaos, escalation, and human burden that follows can be reduced before it spreads.

– Trigger Logic

In the first hour, perfect certainty rarely arrives.
The real question is whether the organisation has defined what is “enough” to act.

Practical resources for CIOs/CISOs

- *Pressure test for leadership control*
- *First-hour containment decisions*
- *Why pressure testing matters*

For readers who want to go further:
I can share more detail on what I mean by the **missing operational layer** — and why that gap becomes so visible when hesitation becomes expensive.

And for teams that want to pressure-test their own setup:
I can run a **free remote resilience assessment** in your own sandbox environment, with your existing security controls enabled, to show how your current environment behaves under pressure and what difference that **operational layer** makes in practice.

If any of these would be relevant for your team, feel free to contact me.

sgemert@s10group.com

- What Delay Costs

When action waits for full confirmation, the incident rarely stands still.
The result is often a wider problem, a heavier burden, and fewer good options.

Sources and further reading

The sources below informed the themes in this newsletter: first-hour authority, ransomware victim impact, clinical disruption, leadership pressure, and the difference between awareness and executable control.

1. NOS
"Als je bedrijf platligt door ransomware: 'Klanten stonden met knuppels op de stoep'"

2. Security.nl
"Brits NHS: ransomware-aanval droeg bij aan overlijden van patiënt"

3. GOV.UK / Home Office & Ipsos
"The experiences and impacts of ransomware attacks on individuals and organisations"

4. VMware / Forrester
"Critical Ransomware Recovery Capabilities"

5. Oxford Academic / Journal of Cybersecurity
"'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organisation's experience"

6. RTL Z
"Massaclaim van start vanwege groot datalek Odido"

7. Politie.nl
"Checkjehack aangevuld met Odido"

8. Odido
"Update over de cyberaanval"

9. Veilig Internetten
"Wat kan je doen na datalek bij Odido?"