



@hrustal via Unsplash: https://unsplash.com/photos/hWuJEL_eYZ4

"Oh sh!t, we've been hacked...": A Case Study Using the Cynefin Framework



Justyn Hornor
Deep Tech Inventor | 7x founder | 5x Patents | Nerd



July 1, 2022

At some point in your career with a large digital product you're going to get that message/call/email that nobody wants, "Oh sh!t, we've been hacked!"

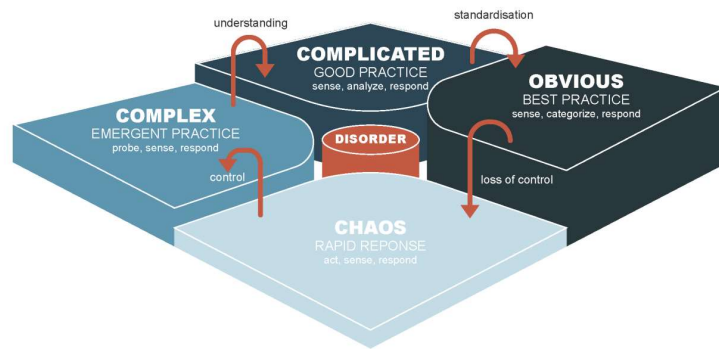
It's at this point that a decision making model, such as the Cynefin Framework, can make the difference between a fast resolution or a complete meltdown. The Cynefin Framework is a "sensing" model for decision-making: the situation can feel like chaos, complex, complicated, or simple.

How YOU feel may be different than others and that's one of the many valuable tools that Cynefin brings to an organization. YOU may feel like a situation is chaos while I think we have a simple process in place to manage it - we may both be wrong, though.

Cynefin Overview

Pronounced Kuh-NEH-vin, this concept was introduced by Dave Snowden in 1999 while working at IBM. Cynefin posits there are four general states a situation may be in:

- Chaos: Unknowable unknowns; act->observe->react
- Complex: Unknown unknowns; solutions emerge
- Complicated: Known unknowns; subject-matter experts weigh-in
- Simple/Obvious: Best practices/SOPs; delegate to people/processes



Cynefin is a "sensing" framework for leaders to determine HOW to make decisions, not what decisions to make. Two parts I won't discuss here are the "confusion/disorder" and "complacency" zones - subsets of the framework that are incredibly valuable but beyond the scope here to go into detail.

Let's look at an example of how getting hacked can expose an organization to an opportunity to apply Cynefin and where leaders can leverage this tool to restore order.

"Oh sh!t, we've been hacked!"

In my distant past I was supporting an organization that experienced a serious breach. In ideal circumstances, the right stakeholders would jump onto the SOC (security operations center) bridge line, we'd calmly ping pong solutions while working in real-time together, and we'd lock down the breach.

No such luck. The org had a Slack channel open with a lawyer, C-suiters, customer support staff, product managers, developers, security staff... There was finger-pointing ("IT told me they had this system locked down!"), left-field recommendations ("Didn't we fire Bill three weeks ago and he had access?!"), too-early-to-tell questions ("Should we put out an email to our customers explaining we've been breached?!"), and so much more.

Chaos -> Complexity

I "sensed" that this was complete chaos. Using Cynefin as a guide, I pulled three subject-matter experts aside and told them, "Look, I might get fired for this, but I want you to completely ignore the main Slack channel for now. I'll run cover. I need you all to..."

This command-and-control leadership style is often necessary in these moments. It can be jarring and risky, but somebody has to make a decision, even if it's the wrong one. Action and clear direction are critical in these moments.

We didn't even know which system was hacked, much less how the breach had occurred. For all we knew, multiple systems had been penetrated. There were too many unknown unknowns. We needed to pick a direction and run fast.

Having isolated the right people now, we gamed out a plan together in our own silo and within a few minutes had a clear sense of what was breached. But we were not sure yet HOW the breach occurred. More research was needed.

Complexity - > Complicated

We're now leaving "chaos" and entering "complexity" - and so my own leadership style needed to shift. I went from command and control to group hypothesizing. How could we quickly experiment to confirm HOW the breach happened so we could lock it down? How could we get some ideas on the table and prioritize? We quickly came up with several systems to go check, divided the list up, and ran down our tasks.

Meanwhile, I was fielding all kinds of conversations in the main Slack thread. It was brutal. People were starting to notice my SMEs weren't responding and beginning to ask questions. I had to own up to the decision to isolate them - which came under immediate fire. "Sorry, team. I need them focused for a few more minutes and I'll give you an update."

At this point one of the team members had confirmed HOW the breach had occurred - we were leaving "complexity" and entering the realm of "complicated." We'd found the issue was due to a 3rd party vendor's lax security on an API endpoint. It was going to take coordinating with several teams internally and externally, but we knew what we had to do.

Complexity -> Complicated

I pulled the vendor's SLA and found the escalation process (thank god we had that documented...), and we quickly had multiple teams working together to lock down the breached endpoint. Within 30 minutes of isolating the team, we'd locked down the breached endpoint and stopped the bleeding.

The subject-matter experts knew what to do and they needed me to get out of their way at this point. They sprang into action and worked closely with the various teams to secure the relevant systems.

Complicated -> Simple

Now we go from "complicated" to "simple" - if you can call fielding the volley furious questions from upset colleagues while drafting a postmortem simple, that is. But everyone knew at this point what was going on and who had which tasks. Our standard operating procedure was kicking in and we all knew our parts.

This process exposed that we should audit our 3rd party vendors a bit more aggressively, so we incorporated this into our ongoing security audit processes. We also decided to war game this scenario at least once a year so we wouldn't end up with another chaos-ridden Slack channel again...

Summary

Cynefin is a decision-making framework that requires leaders to "sense" the current state, make decisions based on the perceived state, and take rapid feedback to determine if they're moving in the right direction. This can be used in almost any situation, but your own leadership style may not be refined for a state such as "chaos" - or worse, you as a leader may think you're always in chaos and treat your organization like a command-and-control scene all the time.

For another layer to this, you can check out OODA loops - Observe, Orient, Decide, Act (repeat) - as a micro-feedback loop for iterating on

information in real-time. It's a common method used in the military and can be incredibly valuable in chaotic situations.

Cynefin gives leaders an extra tool beyond their own decision-making and leadership styles in the moment: probing for how others are feeling at the moment. While you may feel a situation is well-managed, your colleagues may not. Having shared language around how we "sense" a given situation is playing out can be incredibly powerful for organizations.

Lastly, there are two "zones" I haven't discussed: confusion/disorder and complacency. These two areas are important but beyond the scope of a quick LinkedIn post. If there's interest, I can surface how to manage these two zones along with some examples from different industries.

Resources:

- [The classic HBR piece on Cynefin](#)
- [My favorite visualization of Cynefin](#)
- [Video: Dave Snowden, Cynefin's founder](#)

Comments

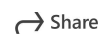
👍 21



Like



Comment



Share

Add a comment...



No comments, yet.

Be the first to comment.

[Start the conversation](#)

Enjoyed this article?

Follow to never miss an update.



Justyn Hornor

Deep Tech Inventor | 7x founder | 5x Patents | Nerd

Follow

More articles for you

