Lean DevOps

A Practical Guide to **On Demand Service Delivery**

Robert Benefield

Lean DevOps

The SolarWinds Sunburst Exploit

The security breaches collectively known as the SolarWinds hacks were caused by a series of exploited vulnerabilities within the IT delivery supply chain. Hackers managed to compromise a build system belonging to the company SolarWinds, allowing them to install malware into updates distributed to customers of SolarWinds' Orion network monitoring tool software. This allowed the hackers to remotely access a wide variety of targets, including the US government.

During this time, attackers also exploited flaws at Microsoft, gaining access to all valid usernames and passwords in each Microsoft network breached. This allowed them to access credentials necessary to assume the privileges of any user, including customer Office 365 accounts. The breach has been so deep that it is unclear as of the writing whether its extent will ever be fully understood, let alone all the damage eradicated.

Modern IT solutions require a better way to assess and manage risk. Rather than continuing to rely upon using compliance processes to find potential hazards and then mitigate their risks, we need to look at what we know about the delivery and operational ecosystem. This includes how much visibility we have into the elements that comprise the ecosystem, as well as the predictability and orderliness of its dynamics.

In this chapter, we will explore how order and predictability affect risk and the decision-making process. We will also cover a number of techniques to help mitigate risks from unknown and unknowable hazards in your ecosystem.

Cynefin and Decision Making

We know that environments can differ in complexity. The more complex and dynamic an environment, the more context and situational awareness we need to confidently make effective decisions in it. However, being

complex and dynamic doesn't necessarily equate to there being more, or more severe, risky hazards. For instance, a meat cutter in a meatpacking plant works in a far less complex environment than a commodities futures trader, yet most would agree that the meat cutter faces a higher risk of injury or death from a bad workplace decision.

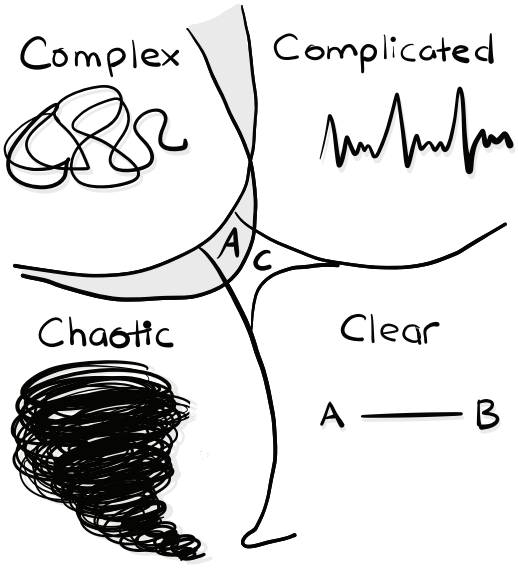
Where there is a difference is in the way that decision risk is managed. While the risks for the meat cutter are more severe, their number is small and well known. Most risks to the meat cutter can be mitigated through scripted procedures that can be closely monitored, such as ensuring that cutting tools are sharp and in good working condition, only using such tools in particular ways, and avoiding slippery surfaces.

The commodities trader, on the other hand, faces a wide variety of ways that seemingly sound decisions can go bad, from bad weather and pest outbreaks to unexpected bumper harvests and political events that dramatically change the supply and demand dynamics of the market. For commodities traders, a scripted set of procedures would do little to uncover, let alone manage, any risks. Instead, they have to constantly seek out the most up-to-date relevant contextual information and adjust their positions within the bounds of their risk tolerance accordingly.

This relationship between contextual dynamics and the suitability of an approach became apparent to David Snowden while working on the problem of knowledge management and organizational strategy. From his work he developed a sensemaking framework called *Cynefin*. His framework is a complexity thinking tool designed to help people sense the situational context in which they are operating in order to make better decisions.[1] Snowden has continued to work and tune the framework, which has grown into a particularly useful guide to help people recognize the dynamics of the domain they are working in and understand why an approach that worked well in one context can fail miserably in another.[2]

1. David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review*, November 2007 https://hbr.org/2007/11/a-leaders-framework-for-decision-making
2. The Cynefin Framework, https://thecynefin.co

Figure 5.1
Cynefin framework.



The Cynefin framework consists of five contextual domains: *clear*, *complicated*, *complex*, *chaotic*, and *confusion*. Each domain is defined by the nature of the relationship between cause and effect, with clear and complicated domains being two forms of *ordered systems*, while complex and chaotic domains are forms of *unordered systems*.

While some environments are more likely to find themselves in a particular contextual domain than the others, any number of developments can raise or lower complexity that shifts an environment into a different domain. This often not only breaks existing risk management but can create delivery friction and cause situational awareness to degrade.

Learning how to recognize which domain your organization is in at a given time can help you find the best approach to manage any risk. It can also be a useful way to spot and mitigate many of the common behaviors that often erode the quality of decision making in them.

Let's take a look at each domain to get a better idea of the different dynamics of each.

Ordered Systems

Ordered systems are those where a particular input or action will directly and predictably produce the same result. This clear and observable relationship between cause and effect holds true regardless of whether specific expertise is required to execute it. As such, the system can be pulled apart and put back together in a straightforward way like a machine.

As you will see, it is the level of expertise required to see the cause-and-effect linkage to make an effective decision that separates the clear and complicated contextual domains. This difference also plays a significant role in how best to manage risk in each.

Clear: "The Domain of Best Practice"

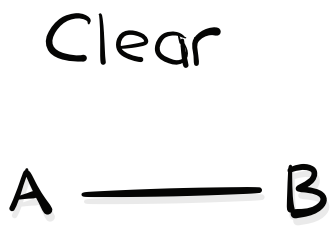


Figure 5.2
The clear domain — simple and obvious.

Clear contexts are those where the problem is well understood and the solution is evident, thus making for perfect situational awareness. Snowden refers to these as "known knowns."[3] The act of problem solving requires no real expertise, just the ability to capture the issue, categorize it, and respond following established practice for the problem category. As the problem is already known, all the work can be scripted ahead of time, either in written form for someone to follow step by step, or as an automated tool that can be activated at the appropriate time.

The earlier scenario of a meatpacking plant is a good example of an ordered system operating in the Clear contextual domain. While an experienced meat cutter might be faster and less likely to get injured than someone

3. Ibid, p. 3

new on the job, there is little discernible difference from the actions of cutting up carcasses of the same type that cannot be scripted.

Clear contexts fit well for Taylorist method-driven management models, introduced in Chapter 2, "How We Make Decisions." Work can be defined and planned well in advance with instructions, coming from the top down, detailing clearly defined best practice. Likewise, risk can be managed by ensuring that workers closely adhere to instructions which explicitly check for known potential hazards, such as the state of tools and surfaces in the meatpacking example. The clear domain is the desired realm of Tier 1 helpdesks and support functions in traditional service management, as instructions can be placed in runbooks that can be searched and followed by the most junior technician.

There are two types of challenges that can plunge a clear contextual environment into chaos that is difficult to recover from. The first danger is that with so much of the actual thinking and directing happening from the top down, it is easy for conditions to shift that cause awareness gaps to form. With people working in such environments so used to following the routine, they often miss the warning signs of an imminent hazard until it is too late to react. Not only is this bad for delivery, the resulting failure and chaos can cause a precipitous drop in worker trust of management that further degrades organizational awareness.

Figure 5.3
Even if the domain is clear, you still need to see it.

There is also a second danger of the people working in the ecosystem becoming so attached to their past experiences, training, and successes that they become blind to new ways of thinking and struggle to learn and improve. Past rules become immutable in their minds, even when evidence of their diminishing suitability builds around them. Established firms that were once successful and large bureaucracies often fall into this trap, forfeiting success to more dynamic or suitable alternatives.

Complicated: "The Domain of Experts"

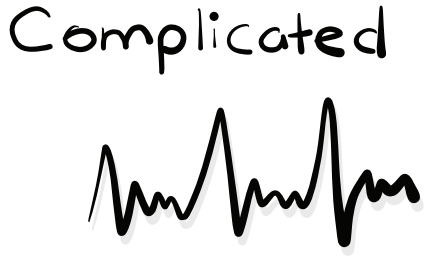


Figure 5.4
Some problems are complicated enough that they need an expert to solve.

The complicated contextual domain is the realm of the skilled expert. Unlike the clear domain, there are enough "known unknowns" that it is no longer possible for management to rely solely upon reusable scripts that an unskilled worker can follow to solve a situation. Instead, some level of domain expertise is required to both analyze what is going on and decide a suitably effective course of action. Typical examples of such expertise include an auto mechanic, an electronics repair person, or an IT desktop support specialist. Likely, all have been trained to match symptoms with known solutions they can confidently execute.

Rather than spending time scripting and enforcing methods, managers break the delivery domain by resource skill type, staffing and allocating tasks according to the perceived demand need. As a result, risk is usually managed through top-down change-gate processes. These are processes that serialize delivery into separate design, development, test, and release stages, each separated by a change management review at the end of each stage where conditions can be reviewed to uncover potential problems that need addressing.