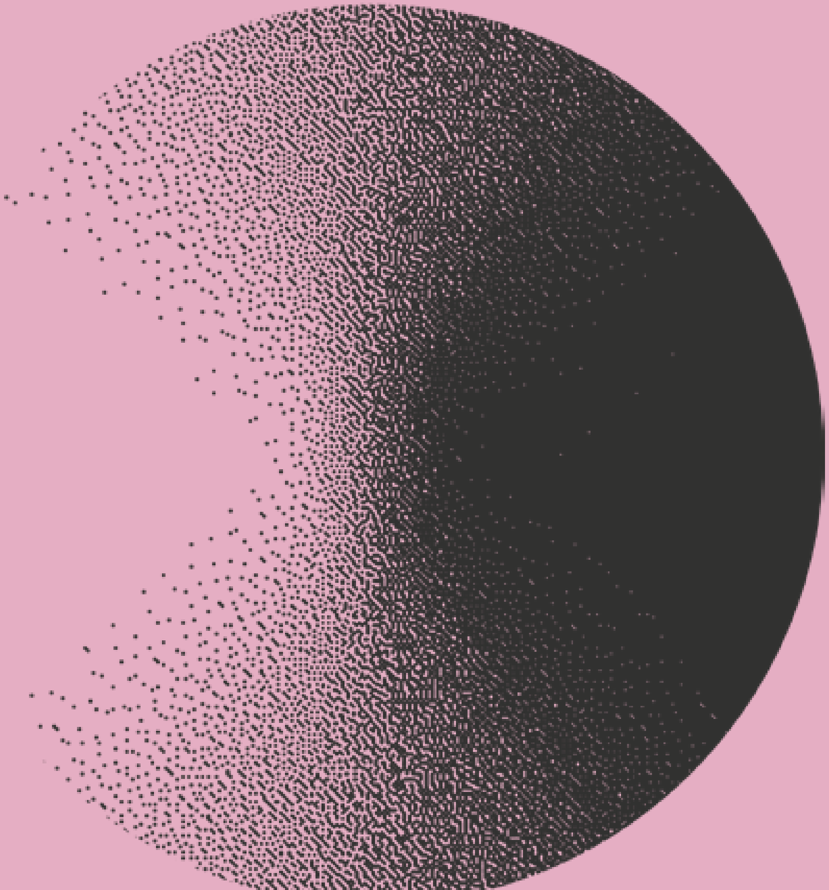
p·d

Shaping

technology

for transformation

Achieving meaningful change starts with the foundations you build.



Contents

Understanding your foundations

Building for adaptability

Designing for resilience

Foreword

Dai Vaughan

At Public Digital, we see user-centred design, a test-and-learn approach, and modern technology practices as the foundations of modern adaptive organisations. By embracing these approaches, organisations can keep pace with evolving customer needs and remain responsive and resilient to change.

When it comes to technology, success isn't about chasing the latest trend. It's about building an organisation's underlying strength - a "muscle" that determines its fitness to compete and survive. This muscle has two critical functions: the adaptability to navigate constant change, and the resilience to withstand inevitable shocks. This isn't a technical problem for engineers to solve alone. It's an organisational capability that grows out of the conditions created by leadership.

Very few organisations are starting with a blank slate. Most have developed layers of systems and processes - what we call "digital geology" - which inhibit speed and agility. This technical reality is often the symptom of a deeper issue: "leadership-debt", which describes the accumulated cost of decision making, generations of frameworks, and outdated ways of working that prevent teams from building the robust, adaptable and modern services they need.

This collection of articles from my colleagues at Public Digital offers a guide to paying down that debt and building your technological strength. From establishing the foundations of culture and ownership, to building the proactive muscle of adaptability, and finally, to embedding the defensive strength of resilience, these articles are designed to take the reader on a journey from merely reacting to urgency and failure to proactively preparing for it.

In today's world, technology *is* the business. Its strength or fragility is a direct reflection of leadership. Building this capability is no longer a nice-to-have, but a fundamental responsibility. That's because in an era of constant flux, achieving meaningful change starts not with what you buy, but with how you build.

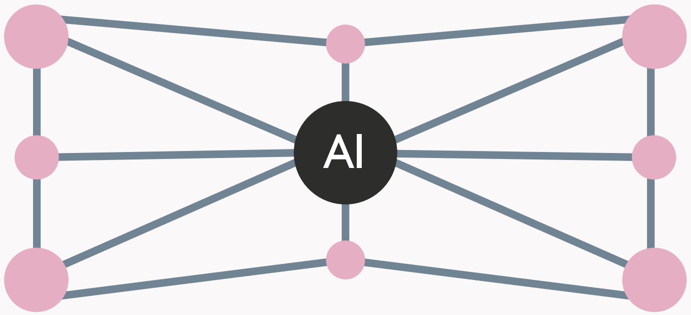
Understanding your foundations

How culture, ownership and decision-making affects your ability to deliver

> You may not consider yourself to be a technologist, but the key to managing technology well is to nurture your curiosity about it.

Digital geology: the layers of legacy of tech slowing your company down

Dave Rogers



The world of technology loves quick fixes and silver bullets. It mythologises rapid disruption and change, powered by the latest technology. 20 years ago, these stories of rapid, leap-frogging change were all about Cloud technology. 10 years ago, Blockchain was the hot new thing. Today, it's Generative AI.

But there's a contradiction. Walk into your average retailer, bank, airline or insurer and you'll find a considerable and accumulating pile of so-called 'legacy technology'. This is the (metaphorically speaking) sticky, stodgy and often smelly technology that sits behind the veneer of modern apps and websites.

In some of the largest, most long-established commercial enterprises, it's possible to find digital technology stretching back to the 1970s. Yes, these same organisations might be testing out Microsoft co-pilot, or experimenting with open-source large language models, but these new, innovative technologies aren't replacing the old. Instead, they're joining them, both forming and rapidly generating the next accumulating layer: a kind of digital parallel of geological strata.

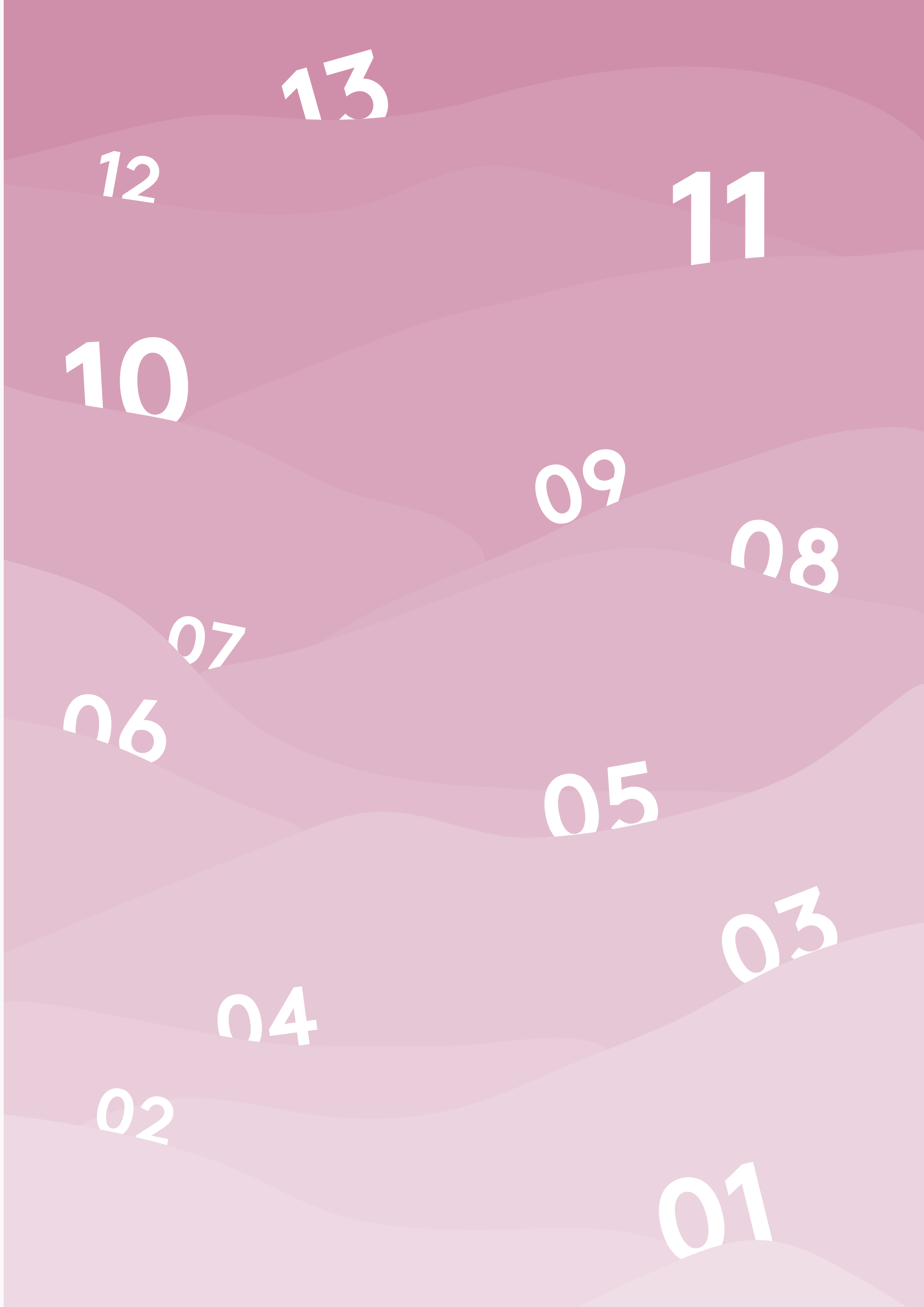
Likewise, the blossoming of the AI age will likely be visible to future generations as a distinctive layer or transition.

Layers of legacy make calamity more likely

Deep layers of legacy technology play a significant role in the majority of major technology calamities. They contributed to the severity of the CrowdStrike-Microsoft outages in July 2024, when a faulty software update from US cyber security provider CrowdStrike prompted global chaos in travel, healthcare and banking. They're why British Airways have suffered from successive IT failures in 2017, 2020 and 2024. They're why the personal data of hundreds of thousands of legal aid applicants in the UK were more vulnerable to attackers, with tragic personal implications and a chaotic impact on legal processes.

The layers, and their impact, aren't always the ancient COBOL mainframes from the 1970s and 80s. The technology of the 2010s is already forming a similar layer for more modern organisations: out-of-fashion javascript libraries such as jQuery, noSQL databases like CouchDB. It was the end of an era for languages like Perl and Tcl, whose popularity has subsequently dropped.

Some digital technologies can globally drop out of fashion and favour within just 2 or 3 years. Vibe coding, where software development itself is accelerated by generative AI, is already creating concern of a newer, yet larger legacy of unmaintained code for future generations to grapple with.



> Outages and hacks are the more visible symptom of legacy, but the slowing effect is what kills companies.

Layers of legacy slow you down

Many organisations have learnt how to work with these layers, and keep their products and services available and secure for customers. But it comes at a cost. The layers slow everything down. Change becomes riskier as the layers deepen. Making fundamental changes, which ripple through the layers, means upgrading and updating fragile IT systems. Those systems can remain in a dormant state for months or years - operating, but in a static, unchanging state.

When a change is necessary, this dormant IT system becomes a source of potentially cascading failure. This kind of change is a leap in the dark with unknown side effects.

Outages and hacks are the more visible symptom of legacy, but the slowing effect is what kills companies. If, year after year, the pace of change is held back, it's only a matter of time before faster-moving competitors can impact revenue. These competitors may simply have the advantage of youth - they've yet to accumulate the digital strata.

How to manage legacy

Crucially, this must be recognised as a hard problem: Large, established companies will have to chip away at this problem year after year after year.

For many companies, the first priority is to slow down the accumulation. The impulse to ship new features and products (over improving, refining, or even reducing what you have) doesn't just "enshitify" - cause the gradual decline in quality of your products - it deepens the layering. Any CTO or CIO offering a quick fix is being falsely certain.

Here are some ideas of how to chip away at legacy layers:

Stop whole lines-of-business

Streamlining your business is an opportunity to instantly drop deep layers of digital legacy. Just as you'd stop a line of business that doesn't make a profit, so you should consider lines of business that have become slow or risky due to legacy.

Be layer-aware

Modern leaders, including CEOs, CPOs and CFOs, need to know about legacy, and have a feel for the age, health and quality of the layers below the surface of the business.

Measure and understand your ability to change

Get better at answering questions like: How long does it take for a new idea to become reality? Do you understand low level metrics like DORA as a measure of engineering workflow?[1]

Find the bottlenecks

Find the parts of your business where legacy has accumulated, the pace of change is slowing, yet you know you need to respond rapidly to changing markets.

Apply creativity to modernisation and simplification

Test the application of generative AI to explore and simplify legacy code bases and documentation. Consider creative services such as Mechanical Orchard who specialise in cutting edge approaches to the modernisation and simplification of very old technology.[2]

Don't reach for big-bang replacement

A common outcome to big bang technology delivery is that your shiny 2.0 sits on top of a decaying 1.0. Instead, take incremental and iterative approaches to changing your technology.

Avoid the legacy skills trap

Legacy technology often demands outdated skills, practice and culture. Don't become trapped in a place where you have the skills you need for your past technology, but too few of the skills you need for your future technology.

[1] pdlink.co/dora-metrics

[2] pdlink.co/mechanical-orchard

> A common outcome to big bang technology delivery is that your shiny 2.0 sits on top of a decaying 1.0.

Stay curious

You may not consider yourself to be a technologist, but the key to managing technology well is to nurture your curiosity about it. Look beyond silver bullet solutions, learn about modern tech practices, examine the technology as experienced by your staff, your makers, your operators and not just your users.

While it can be tempting for leaders to delegate complexity and specialism, taking this approach to legacy technology is profoundly risky: your layering of technology is probably growing, and probably slowing you down.

The approach you take could well determine the fate of your business.

Avoiding the hidden costs of leadership debt

Oli Lovell

In technology, there's a hard truth: systems don't stay still.

User needs, technology and security threats change constantly, and so the systems in an organisation which govern or respond to them must change too. You're either investing in those systems - for better or worse - or you're decommissioning them.

> As a leader, your skills, models and culture operate as a system of their own, determining how well your organisation is able to adapt and respond to change.

The cost of standing still

When it comes to technology, the failure to decommission and reinvest in up-to-date systems can lead to technical debt - meaning the natural degradation of technical capabilities. Over time these legacy capabilities become more brittle and expensive to maintain, as well as increasingly tangled and complex. They slow the pace at which new systems can be deployed, and become a hidden liability on the balance sheet.

Technical debt is well recognised. But the same logic of ever-shifting organisational needs - and therefore the debt accrued by standing still - applies to leadership too. As a leader, your skills, models and culture operate as a system of their own, determining how well your organisation is able to adapt and respond to change.

And if you're not actively investing in those leadership skills and behaviours, you should be decommissioning them.

Leadership debt

Leadership debt is no less toxic for organisations than technical debt. It is the accumulation of outdated mindsets, behaviours and decision-making frameworks that prevent an organisation from adapting at speed.

Just as inactivity leads to muscle atrophy, leadership debt causes the organisational muscles for adaptability and resilience to weaken, leaving the business brittle and vulnerable.

Over time this can:

- Create a brittle culture which is risk-averse and resistant to new ideas
- Prevent innovation: valuable staff who practice new ways of working become blocked or leave.
- Become a drag on speed and morale: Slow decision-making frustrates empowered teams and slows delivery.
- Become a hidden, growing liability: The organisation gets slower, loses talent and fails to meet user needs.

What to decommission: a to-do list for reducing leadership debt

Like technical debt, leadership debt often happens unconsciously, through continuing to use systems or behaviours that are slowly but surely becoming unfit for purpose.

Avoiding leadership debt requires a sustained, conscious effort to identify and decommission what is no longer working in your leadership approach, and actively invest in approaches that will enable your organisation to become adaptive.

This will be specific to your context, but the following guide serves as a starting point for leaders:

Decommission: Layers of governance and oversight as the primary decision tool.
Invest in: Decisions made by empowered teams, based on user research and data: As close as possible to detailed, current knowledge.

Decommission: Big-bang, multi-year strategic plans that are obsolete on arrival.
Invest in: A clear strategic intent, executed via incremental test and learn cycles.

Decommission: Leadership as a function of control and reporting.
Invest in: Leadership as a service to teams - providing context, removing blockers and creating psychological safety.

Decommission: Rewarding delivery of outputs (the "what").
Invest in: Rewarding the achievement of outcomes (the "why").

Decommission: Telling people what to do and when to do it.
Invest in: Storytelling. Creating compelling stories to change and inspire.

> Your leadership approach is either an asset you are actively improving, or it is a legacy system accruing debt every single day. It cannot stand still.

There is no middle ground

Your leadership approach is either an asset you are actively improving, or it is a legacy system accruing debt every single day. It cannot stand still.

This is not about being a "bad leader". It's about recognising that the context has changed, and the old playbook no longer works. The world moves; you have to move with it.

Moving from a command model to a coaching model, from directing to enabling, is hard work. It requires a conscious, sustained investment.

If you are a leader ready to pay down this debt, the first step is to recognise it. The next is to begin the hard work of building new capability. The following chapters provide the plan for building the organisational muscles required to create a truly resilient and adaptive organisation.

Building your company's digital sovereignty

James Stewart

The term 'sovereignty' usually belongs to the language of politics. Recent geopolitical and trade shifts have shown the extent to which countries rely on one another for digital services, and explain the appeal of 'technological sovereignty' as an ambition for governments.

But these issues aren't exclusive to government. They apply to everyone who provides - or even relies on - digital services.

Defining digital sovereignty

At Public Digital we define digital sovereignty as:

> "The agency and capacity of any organisation to make intelligent, informed choices to shape its digital future by design."

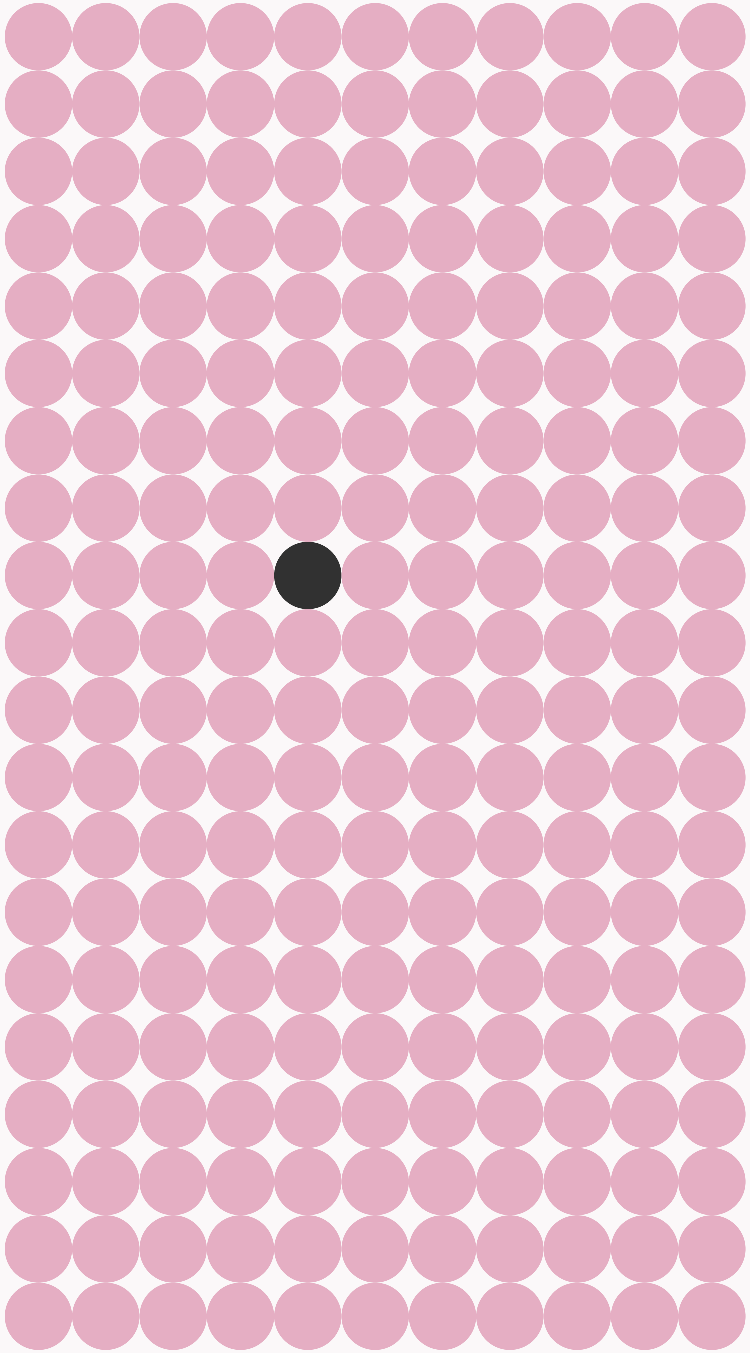
That means having a handle on the risks to how you operate now (are you able to comply with evolving regulation, are your bills going to escalate because of tariffs or exchange rates, will services you depend on remain available to you) but also the ability to shape your own future. It's about ensuring that you have control of the right things, and a strategy to ensure you don't become overly locked into the constraints created by markets or particular players.

As my colleague Mike Bracken has spelled out, we see real digital sovereignty as having two crucial components - agency and capacity:[1]

- Agency is the power to set a direction. It is the ability to act, to make a deliberate decision, rather than being forced down a path by circumstance. This calls for leadership confident enough to question its existing digital estate and to explore alternatives, even when the default path seems easier.
- Capacity is the institutional competence to choose well. It means having the skills, processes and knowledge to make sense of your digital geology. It goes beyond just having technical talent. It requires leaders who grasp how digital systems work, procurement teams who can design contracts for the digital-era, and policy makers who understand the strategic implications of different technology choices.

Significantly, this also means ensuring that how you understand technology is a central pillar of your strategic decision making, not an afterthought, especially in times and areas of uncertainty.

[1] pdlink.co/digital-sovereignty



If you lack understanding and control of your digital systems, you lose your ability to respond to customer needs and your ability to guarantee a high quality of service.

The dual risk of inaction

What are the risks of ignoring digital sovereignty? There are two sides to this, both equally vital for the C-suite to grasp:

1. The geopolitical and supply chain risk. As sanctions regimes change, and tariffs or export controls are introduced, you may find that services you depend on are harder to access, are increasingly expensive, or carry new risks. Large organisations must keep an eye on this kind of big picture volatility.

2. The operational and customer risk. At a more immediate level, if you lack understanding and control of your digital systems, you lose your ability to respond to customer needs and guarantee a high quality of service. This loss can be existential for any organisation. As we've seen with recent cyber attacks, organisations that are locked out of systems with no plan for a minimum viable alternative face catastrophe.

Not independence, but intelligent dependence

In 2013, Dr. Werner Vogels, Amazon CTO, cautioned against what he called “undifferentiated heavy lifting.” He was referring to the fact that an increasing amount of both the technology that we need to do business and the technologies that we need to provide distinctive services was readily available for re-use. His comments were a sound challenge then and remain one now: we still encounter too many organisations investing too much effort or money in low value activities.

But this approach can also be the start of a slippery slope. Just as wholesale outsourcing strips organisations of agency, so too can thoughtless reliance. The challenge of technology leadership and architecture is how to minimise the undifferentiated work, but maintain the agency to adapt as your business and the operating landscape change.

The goal is not an unattainable ideal of ‘digital independence’. The goal is intelligent dependence.

Herman Hauser, founder of chip designer ARM, offered a useful framework for assessing this capability, which can be applied directly to commercial entities. For “countries,” insert “companies”:

> “Do I have all the critical technologies myself? If not, do I have access to these critical technologies from a number of countries to avoid being overly reliant on one? And if I do need to take support from a monopoly, do I have guaranteed unlimited access to those technologies? The answer to at least one of these questions must be yes, or else one risks real dependency.”

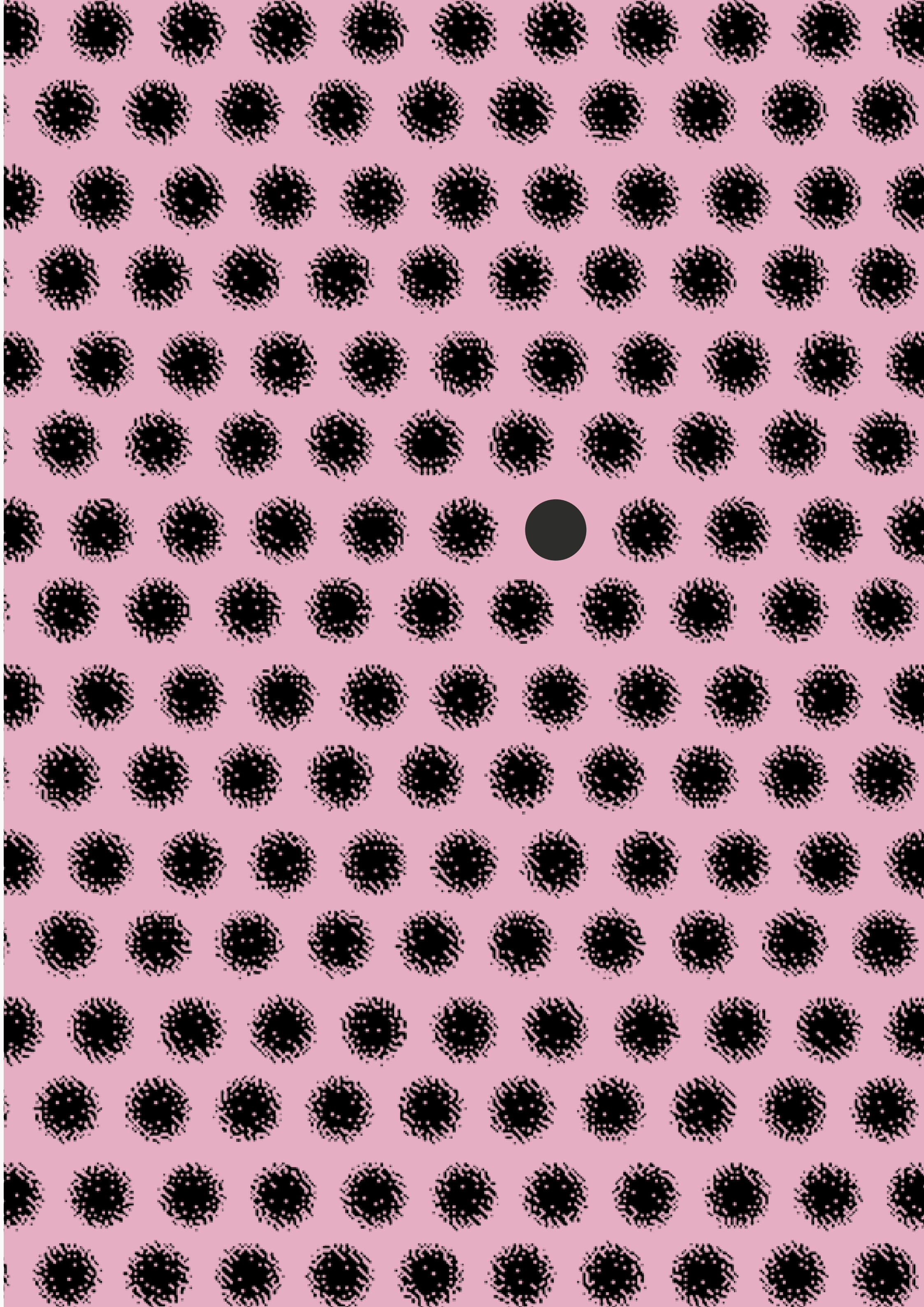
Parts of Hauser’s challenge are a tall order for almost any organisation, but the challenge is useful. It forces us to think clearly about how we’re set up, what we’re going to need, and how to build toward that: from developing our own skills, to investing in open source options, to active acceptance of some risks.

How to build sovereignty

1. Understand your status quo and the forces that have shaped it

A huge part of this work is in building situational awareness, and this has two critical parts:

- Understand the market. Your organisation must have a thorough understanding not just of the market you sell into, but of your technology supply chain.
- Understand internal operations: Many organisations have outsourced so heavily that nobody in-house understands how your operations work. This is equivalent to buying what you don't understand.



2. Know where your greatest costs of change are and (if you're not comfortable with that) work to reduce them

Situational awareness naturally leads to mapping out what you're dealing with, which helps you identify areas where your control is low. Once identified, you can determine if that low control is acceptable, or if you need to carve out a strategy to change it. This might mean introducing multiple vendors for something where you've only got one, or investing in an open source solution to run alongside something commercial to ensure you always have options.

Most of the work you need to do is not radically new. Over the past 15 years, practices like shifting to the cloud, building automation, collaboration, and rigorous testing (DevOps practices) provide a strong foundation. Making these investments significantly reduces your cost of experimenting with a second cloud provider, or attempting to run services side-by-side.

3. Avoid the common pitfalls

Leaders often make two crucial mistakes:

1. Thinking purely technologically. As soon as you introduce the word *digital*, people tend to think purely about a technology solution. However, by thinking more broadly about business operations and business priorities, you create more options for yourself. For instance, a short-term crisis can be managed by changing a business process or moving to a manual process.
2. Focusing only on data location. While regulators and customers may demand data location, this is not the start and end of your sovereignty conversation. You are not "fine" if your data centre is local but all the software running in it comes from elsewhere. You must think holistically about what is needed end-to-end.

4. Actively shape your market

The choice for leaders is not a simple binary of "build vs. buy", or a battle between a few dominant providers.

Large organisations have significant power to influence their own supply chains, but even smaller ones can act. If you're dissatisfied, it's likely that others are too - together you can have leverage.

> A core part of being able to be sovereign is having clear multidisciplinary teams who are responsible for the holistic outcomes of services.

5. Get the right people at the table

The sovereignty conversation is not just a technology conversation. It overlaps significantly with cybersecurity and general business strategy. The entire leadership team must collectively define the organisation's priorities in what it is able to control, guarantee, and rely on.

A core part of being able to be sovereign is having clear multidisciplinary teams who are responsible for the holistic outcomes of services. This means teams thinking about the technology, the users, the business outcomes and the non-digital operations that go behind it - all together. These teams are what enable you to respond to change.

Underneath the C-suite, you need representation from all disciplines across the business, working together to create a holistic understanding of how you work now, and how you want to work.

Sovereignty isn't the end goal

Simply having agency isn't enough. The important thing is what we do with it. But without agency, we lock ourselves - and those who depend on our services - down. We limit the problems we can solve and the ways we can solve them.

It is within every organisation's power to increase their agency - and their sovereignty - and it has never been more essential.

Building for adaptability

How to build the capability to thrive on change, not just survive it.

> In a world where technologies and markets move quickly, being able to learn what works and adapt accordingly is the single biggest factor in organisational survival.

Building an adaptability muscle: the foundation for the AI era

Dai Vaughan

Today, the emergence of generative AI represents not just another incremental step, but a profound acceleration, moving at a speed that makes the internet era feel slow. The landscape of tools, capabilities, and customer expectations is shifting daily. It's natural to feel that just as you're learning the rules of one game, another has already begun.

As leaders, we often focus on managing technical debt. But in an era of constant change, the most dangerous liability we carry isn't in our legacy code - it's in our legacy ways of working.

We've seen how this manifests as both a technical liability as 'digital geology' and a cultural one as 'leadership debt'.

The way we build and operate technology has undergone a seismic shift in the last two decades. A relentless cycle of new technologies demands our attention, forcing us to adapt how we design, build and operate. The internet era forced a fundamental rethink, introducing concepts such as agile, multidisciplinary teams, and DevOps. For many established organisations, this is a difficult, foundational shift that is still in progress.

While the methods have changed over time - from waterfall to agile, from on-premise to cloud - one factor has remained constant: the ever increasing velocity of change.

This creates a fundamental question for leaders: how do you prepare for a future that is arriving faster than ever? The answer is not to bet on a single technology, but to build the right capability: an institutional "adaptability muscle" - the organisation's enduring capacity to adapt to relentless change.

This isn't the first time our industry has faced a crisis of speed. The blueprint for managing this new velocity of change was written over the last decade, and its lessons are more urgent today than ever.

> The success of internet-era giants didn’t come from a specific tool, or a better technology, but from having a better operating model to manage change.

A case study in silos and speed

In the early 2000s, the technology operating model in most large organisations was defined by conflict. Development teams were incentivised to create new features, while Operations teams, focused entirely on stability, fostered a defensive culture of “No”. This tension resulted in a technical ‘brittleness’, where every small change risked breaking the entire system. The natural outcome was friction, slow release cycles, and a culture of blame. It was a model that could not keep pace with the demands of a connected world.

The response was a fundamental shift in mindset: DevOps. This was not merely a technical fix, but a cultural one. It brought teams together around a shared purpose: delivering value to users. This new approach broke down silos and introduced more fluid ways of working, such as Continuous Integration and Continuous Delivery (CI/CD), enabled by the automation of cloud computing.

Internet-era giants like Google and Amazon, and even pioneering government teams like the UK’s Government Digital Service, mastered this approach. They built multidisciplinary teams that could deliver improvements not in months, but in days or even hours.

Their success didn’t come from a specific tool, or a better technology, but from having a better operating model to manage change. They mastered the underlying principles of delivering value for users: creating multidisciplinary teams, building automated pathways for safe deployment, and fostering a culture of shared ownership. It is these principles, not the specific tools of the past, that form the blueprint for adaptability today.

Adaptability is your best defence

An adaptable organisation isn't just faster - it's more resilient, with the ability to react effectively when things go wrong, regardless of the cause. The COVID-19 pandemic provided a stark, real-world test. Organisations with well-developed adaptability were able to pivot in weeks, scaling digital services and supporting remote teams because their culture and technology were already built for change. Those with rigid structures struggled.

This resilience is also critical for navigating the fragility of our modern technology ecosystem. Often, the greatest risk comes not from external threats, but from within. A single, flawed software update - an accidental failure - can cascade through interconnected systems, causing outages which are just as damaging as a malicious attack.[1]

This is where the ability to react at speed becomes a vital defensive capability. An adaptable organisation can quickly diagnose, patch and deploy a fix, whether the vulnerability is from a cyber attack or an internal error. This capacity to recover quickly is a direct outcome of a culture that values collaboration and invests in automation - the evolution from DevOps to DevSecOps. In the modern era, resilience against all forms of disruption is a vital part of effective risk management.

[1] pdlink.co/accidental-tech-failure

Adaptability is a competitive advantage

Beyond resilience, this operational fitness gives organisations a profound competitive edge. While non-adaptive competitors are encumbered by their legacy systems and processes, an adaptable organisation can pivot when the market shifts, seizing new opportunities. They can adopt more efficient technologies as they become available, replacing legacy components without massive disruption or multi-year programmes.

They can, in short, operate "by design, not by default," continuously choosing the best path forward rather than being dictated to by the limitations of their past decisions.[2]

[2] http://pdlink.co/digital-sovereignty

> The focus must shift from finding the “perfect” AI strategy to building the core muscle that enables safe and rapid experimentation.

The impact of AI: adaptability is non-negotiable

If adaptability was an advantage in the internet era, it has become non-negotiable in the AI era. AI tools allow teams to build and test prototypes in minutes, not weeks. New services and models with new capabilities are appearing daily. It is impossible to predict which of these will prove most valuable.

Chasing every new trend is a recipe for burnout and wasted investment. As we have argued before, simply plugging new technology into an old operating model leads to disappointment.[3]

The velocity of change is now too fast for long, drawn-out analysis. To thrive, organisations must adopt a prototyping mindset at scale. This demands a commitment to continuous learning, where teams are not just encouraged to try new things, but are also empowered to unlearn the old habits and processes that no longer serve them in this new context.

Where an agile mindset helps a team respond to changing customer needs, an experimental culture allows them to test ten different AI approaches to find what delivers real value. Where a collaborative structure helps launch a new digital feature, it also enables the organisation to safely explore and scale opportunities from new AI prototypes.

The focus must shift from finding the “perfect” AI strategy to building the core muscle - the people, processes, and platforms - that enables safe and rapid experimentation.

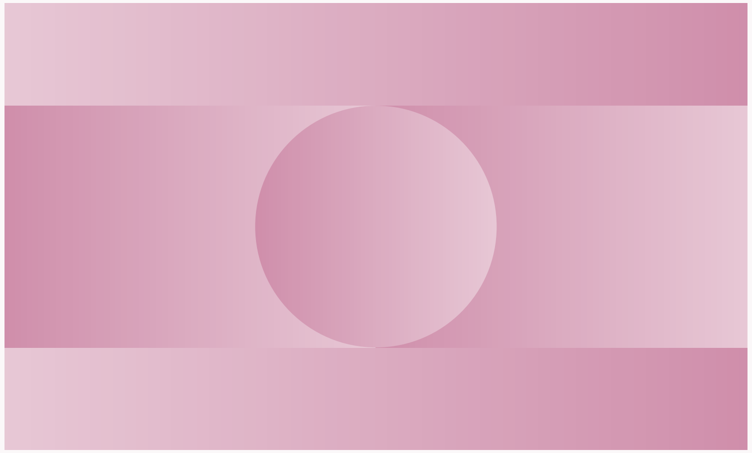
[3] pdlink.co/new-tech-old-state

How to build adaptability

Developing this adaptability muscle is the most critical work for leaders today. It shifts the focus away from reacting to each new wave of technology, and towards the deliberate work of building a resilient foundation for the future. It is the direct investment you need to make for whatever comes next.

This begins with asking honest questions, and then applying a test and learn mindset to answer them:

- Where does our current structure create friction and slow down good ideas? A test and learn approach means starting small: instead of launching a large, high-risk programme, identify a single, meaningful challenge and focus the first effort entirely on a clear learning objective.
- Are we empowering our teams to solve problems, or preserving a culture of top-down control? True empowerment comes from decentralised decision-making. Give a small, multidisciplinary team the autonomy and context to solve the problem, trusting them to make choices quickly without needing to escalate through a complex hierarchy.
- How can we create safe spaces to experiment and learn? This requires a genuine commitment to psychological safety. Leaders must create an environment where a failed experiment is treated as a successful lesson learned, not a punishable mistake, ensuring that valuable data is never hidden for fear of blame.



Start small

The most practical first step towards building adaptability is to start with an exemplar project and take a test and learn approach to solving it. Public Digital's book on Adopting the Practice of Test and Learn - the second in our series of three - explains how to take that practical first step.[4]

For any organisation, building this foundational adaptability is the most effective way to prepare for the future. Your competitors who possess this capability will build faster, weather risks more easily, and leapfrog those who don't.

In the AI era, building this muscle is what transforms the daunting pressure of constant change into a sustainable, competitive advantage.

[4] https://public.digital/test-and-learn

Untangling your technology spaghetti

Dai Vaughan, James Stewart

Many of us have had the experience of asking for something simple - a change in colour scheme, some extra data insight, or what should be a quick experiment - and hearing 'that's complicated'.

In many established organisations, the biggest blocker to meaningful change isn't a lack of new ideas - it's the complex legacy technology at their core.

This problem has a few names. You might see it as "deep digital geology" - brittle, immovable layers of outdated code and infrastructure, built up over decades. Or you might see it as "technology spaghetti" - a critical, tangled-up mess of systems, data and processes where pulling on one thread risks breaking something else entirely.

Both metaphors point to the same truth: this complexity is not static; it gets worse over time. When you want to do something new, the easiest path is often to add another system on top, aggregating the new on top of the old. This problem is compounded as time passes: people leave the organisation, understanding fades, unmaintained systems get forgotten, and change gets harder.

For a leader, this is a strategic trap. You want your organisation to be agile, to respond to market shifts, or to deploy new tools like AI, but every new initiative gets bogged down in this brittle foundation.

The common "big bang" rewrite is fantastically expensive, high-risk, and often fails.

This article offers a different, more practical path: an iterative way to untangle the mess and build a more adaptable future.

Setting yourself a goal of continuous untangling

You don't untangle a knot by pulling on every thread at once - you'll only make it tighter. The solution with your knot of "technology spaghetti" is to start a *continuous practice* of untangling.

This is more than just an IT clean-up exercise. Creating a long-term goal of continuous untangling gives your organisation the opportunity to focus strategically on how you use technology to deliver value.

What's more, this practice is what builds your organisation's adaptability muscle. Like any muscle, it starts small and grows stronger with consistent, focused effort.

The real work of untangling depends on the application of modern technology practices: describing infrastructure in code, a broad range of automated testing tools, and the culture of continuous delivery.

Here are some ways to start:

1. Map and measure your spaghetti

You can't untangle what you can't see. As a leader, you must work to build a clear map or register of your technology. This isn't just a diagram; it's a living inventory that tracks what a system does, who owns it, and when it was last updated. This allows you to quantify the cost of failures (in lost productivity or failed customer transactions) and set measurable targets to reduce them.

2. Start with a user-need thread

With your map and your metrics, you can now pick the right thread to pull. Don't start with the oldest or ugliest tech; start with the most critical user journey that is made slow or painful by your technology. This focuses your effort on immediate business value, which builds momentum and buys you the political capital to continue.

3. Create flexible "seams" to build around the old

Empower your teams to build around the core, not just replace it. The tactic is to first create "seams" in your legacy systems using APIs (Application Programming Interfaces).

These APIs act as safe, modern "sockets" that allow new services to plug into old data and processes. This gives you the flexibility to untangle and replace one strand at a time - or build something new on top - without having to break everything else it's connected to.

4. Master the art of stopping

Untangling and building around is only half the job. The most unglamorous yet most powerful part of building adaptability is **decommissioning** - intentionally stopping and removing the "dead threads" of spaghetti that are no longer needed.

This is often seen as a cost with no "new" feature to show for it, and is perceived as pure risk.

But this practice of "knowing when to stop" is the only way to truly reduce your risk, lower your maintenance costs, and free up your most talented people. This is not just a technical clean-up task - it is a difficult strategic capability that is fundamental to building a truly adaptable organisation.

> Rather than being a project you complete, legacy modernisation is a permanent capability you build.

The spaghetti is never truly tangle-free

Rather than being a project you complete, legacy modernisation is a permanent capability you build. It's important to remember that none of these objectives can be met overnight, and none of them are ever really finished

In a healthy organisation, there will always be change, and there will always be cycles where complexity grows and then diminishes. That's okay, as long as it's recognised and managed.

Focus on something you need to get done - a new capability in your product, a new insight you want to capture, a process that needs to be clearer - and work on it. But at the same time measure whether you've made the system simpler (less tangled) as you've gone. Will each change make the next one easier to do well?

This iterative cycle - of stopping new tangles, mapping the old, pulling on key threads, and removing what's dead - is the "adaptability muscle" in action. It's how you methodically transform your organisation's foundation from a brittle, tangled mess to an orderly platform that is, by design, built to evolve.

Adaptability means knowing when to stop

Julia Harrison

Deciding to stop what you're doing can feel like failure.
In reality: it's not.

For your business to be adaptable, stopping things is essential.

You might realise a product isn't going to work early on - perhaps even at the prototype stage. Or after many years of dependable service, a once-successful product might have ceased to be as valuable as it was. Either way, stopping or shutting something down when it's no longer viable is a healthy decision, and making that choice in good time is something to celebrate.

One major benefit is being able to recover the opportunity cost: When you stop spending time and energy on propping up low-value products, you free up capacity to focus on your real, strategic priorities.

But more importantly, in a world where technologies and markets move quickly, being able to learn and adapt quickly is essential to survival. This shouldn't be limited to sandboxed teams of mavericks and people with "innovation" in their job title. To develop this test and learn organisational muscle, you need a culture where stopping things is normal.

Why stopping is hard

Our decisions are influenced by powerful forces which can make retiring a product or even stopping an experiment feel deeply uncomfortable:

The sunk cost fallacy

The illusion that something is worth continuing purely because you've invested so much in it is a very compelling one.

A way to counter the sunk cost fallacy is to ask: "If you didn't own this product today, would you buy it?". If the answer is no, then it's time to stop.

Bad feelings about sunk costs are real and shouldn't be ignored. It can help to remember that building and running something, whether it's a prototype or a mature service, inevitably teaches you valuable lessons you couldn't have learnt any other way. Whatever those lessons are, but especially when the lesson is "this isn't going to work," you can either act on what you've learnt or carry on as you were. Which is the sensible choice?

Business-as-usual

In many organisations, leaders and teams are culturally - and materially - incentivised to keep working on a product, regardless of its value.

Even when the reality is obvious - whether it's a product outmatched by a market competitor, or a service underpinned by technical debt which has slowed progress to a snail's pace - it is often easier to stick to the status quo.

The risk factor

Ending a piece of work often triggers uncertainty. For both teams and leaders, stopping or shutting something down can carry:

- Risk of the product being seen as a failure, damaging career prospects, remuneration, or job security
- Risk of damaging relationships, whether it's customers, internal stakeholders, or colleagues
- Fear of the unknown: If we don't carry on doing the thing we're familiar with, what happens to us?

These fears can deter people from sharing - or even interrogating - the true picture of a product's viability.

How to develop a healthy approach to stopping

In many cases, the people closest to the work will have known for a long time that a product has ceased to add value. The lag from it being 'common knowledge' (if you talk to the right people) that something is doomed, to a decision to do something about it, can be huge. As can the associated costs.

But the fears which prevent that information from being surfaced and acted upon - like the forces which promote maintaining the status quo - are valid, and demand serious attention.

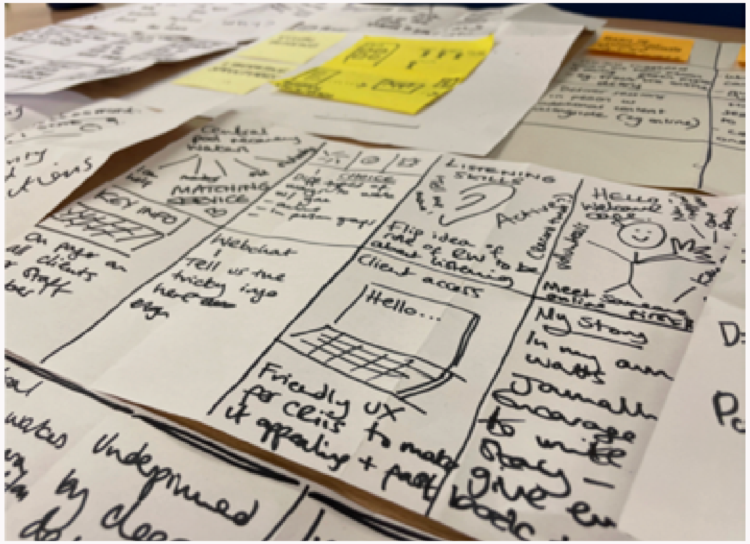
To build a healthy approach to stopping within your organisation, here's what you need to do:

1. Commit to and align around top-level priorities

The ability to deliver strategic objectives depends on all senior leaders committing to a set of shared priorities, and demonstrating that commitment through their actions. Stopping things is no different.

When a decision to stop something in one part of the organisation impacts the ability of another to meet their goals, this naturally creates conflict. This often results in a sense of "us vs them" which cascades down to team level with damaging effects. It's only through commitment at the executive level that these difficult decisions can be made, and made right - for instance by changing a sales target in one area so nobody is penalised for a decision which benefits the organisation overall.

> Success is learning as much as you can, which might not mean a viable product at the first attempt, or even the second.



2. Build a culture focused on learning

Rather than embarking on projects with the assumption that they will succeed, treat each one as an experiment with a hypothesis which might be supported or falsified. Success is learning as much as you can, which might not mean a viable product at the first attempt, or even the second.

This test and learn approach means abandoning false certainty and acknowledging upfront what you know and what you don't. For each new piece of work, teams need to ask:

- What problem are we solving, for whom?
- What's our hypothesis for how we might solve it?
- What are the quickest, cheapest ways to test that hypothesis?

Followed by:

- How will we know when we need to change direction?
- How will we know when we've solved the problem?
- How will we know when it's time to stop?

Leaders need to support this fundamental shift in approach through their actions: by showing they are receptive to new information, and taking accountability for acting upon it. Disincentives to adopting these new leadership behaviours, at any level of the organisation, must be surfaced and challenged.

3. Create psychological safety

For the above to work, people need to be able to challenge the status quo, embark on experiments, and share uncomfortable truths without fear of repercussions. That demands a culture of trust and respect - not one of blame.

Bringing a service or experiment to an end should trigger a retrospective, where teams share the lessons from what went well and what could be done differently next time. Instead of asking who is responsible for the failure and what should they have done to avoid it, start by acknowledging the benefits of stopping now rather than not later, and then ask: "Could we have learnt earlier that this wasn't working?" and "Could we have learnt the most important lessons with a smaller investment or less fallout?".

Leaders must show confidence in the teams who share difficult news by listening to them, supporting them, and celebrating the people who took the courageous step to say "this isn't working".

The work of creating something new inevitably involves learning. The only real failure is in failing to use what you learn.

4. When it's time to stop: practice openness

News of a decision to shut something down can be difficult for teams to hear, particularly if a service has existed for a long time. But continuing to work on something which doesn't add value is also a drain on morale. If the message is delivered well, apologies aren't necessary, but people deserve to know how the decision was taken, and why.[1]

Leaders need a confident, well-reasoned narrative which brings teams with them: explaining transparently what information led to the decision to stop, what they have learnt, and how this experience has strengthened the organisation. They can then begin to energise people around the valuable challenges they will have the opportunity to work on instead.

[1] http://pdlink.co/obstacles-to-shutting-down

> Failure to develop the practice of stopping means failing to develop a critical muscle in learning and adaptability.

The risk of *not* stopping

Whether it's down to the gravitational force of the status quo, the potential threat to jobs and relationships, or a fear of the unknown, shutting something down often feels profoundly risky.

But continuing to pour resources into the slow decline of products which don't add value is bad business. It prevents you from pursuing new, potentially transformative products or services.

It may feel risky, but stopping is your only alternative.

More fundamentally, failure to develop the practice of stopping means failing to develop a critical muscle in learning and adaptability. In a fast-changing world, that's the greatest risk of all.

Good portfolio management to support thriving teams

Matt Harrington

Within a large organisation, digital transformation involves multiple separate projects happening at once, led by different digital teams and overseen by a portfolio office. The system for managing those projects will vary from organisation to organisation, but is likely to involve coordinating regular progress updates from each team, perhaps through a shared spreadsheet or a cycle of meetings.

Done well, portfolio management can bring real value to the projects it oversees. But it is hard to get right.

As with a great deal of bureaucratic systems, this function has a tendency to become focused on metrics, taking the form of a simple reporting process rather than something value-adding. Individual teams may do excellent work measuring their own progress only for a manager to demand metrics of progress from all teams in a generalised format. Forced into boxes on a spreadsheet, this information brings little value to a general overseer, and wastes the time of the project team.

Instead, leaders must shift from policing and blocking teams to enabling them - leveraging their unique ability as portfolio managers to handle pressure, solve problems, and provide support.

When reshaped into this active, enabling overseer, the portfolio office becomes the central nerve centre - the *mechanism* - for building your organisation's adaptability muscle at scale.

The following tips provide a practical guide for how to get it right.

Be outcome-focused

Progress should be measured in outcomes, not focused around milestones. Asking teams to show they have met a particular target by a particular date ignores the ambiguities not captured by a set of dates in a spreadsheet. It also risks missing the point of the work being done.

Be data-focused

Using data, not deliverable milestones, is the most effective way to assess outcomes. Measuring against tangible outcomes expressed through evidence provides the strongest indicator of what has been achieved by a team over a period of time.

Don’t fuss over detail

Good portfolio management is high-level, and draws out the key issues, rather than getting stuck in the weeds. A small delay to a deadline, for instance, is not worth getting caught up on compared to the resourcing pressures on a team, or a problem which has already been solved by a different part of the organisation.

Think hard about reports

If there must be a reporting cycle in your portfolio management, do the hard work early of configuring which metrics will make that report most useful. Consider the type of information that will translate meaningfully into a report and provide value to the portfolio office. That means devising a new report tailored to each new project, not using copies of old ones.

Create a feedback loop

One easy trap to fall into with portfolio management is a ‘feed the beast’ approach: teams hand in the necessary paperwork to their portfolio office in order to be left alone and allowed to get on with the proper work. This one-way system is limiting, if not counter-productive. Portfolio management systems need an embedded two-way feedback loop, where teams can raise feedback, ask questions, and highlight issues.

Go to the show and tell

If you’re struggling to understand something in a team’s report, don’t ask for more paper. Instead, go and see the project and its team: let them show you the work they’ve done. Providing that teams are able to work in a way that invites a ‘show and tell’ approach, seeing the latest outcome of their project will give you a far greater insight than having something written down on a piece of paper.

Don’t be the project-police

Policing your teams will prove less fruitful than assisting them. Think of them as partners to the portfolio office, and share accountability for delivery. Plan your work around how you can best provide support and help them overcome challenges.

Don’t be a post box either

A portfolio office is not a post box for reporting, nor a body for date-checking. To see it this way ignores its unique potential as an active overseer. The position of the portfolio manager as the nerve centre of all these projects gives you access to the collective insight and tools of the entire organisation. A portfolio office is a hub for joining up this knowledge.

Above all, focus on useful conversations

The gift of oversight unique to the portfolio office allows you to spot patterns. You can see where there is demand for the same resource. You can see where one team is struggling in an area that another team mastered earlier on. Or where both teams are struggling with the same problem, and where a collective solution would address that problem. A core responsibility of the portfolio manager is to identify those patterns, help resolve issues, and facilitate communication and knowledge-sharing between teams.

> Shifting the function of the portfolio office from one of policing to one of enabling is precisely how you build that muscle.

Thriving teams are the key to success

Portfolio management is complex. It involves juggling multiple responsibilities at once: escalating cross directorate risks like capability and recruitment, creating a delivery narrative, managing demand pressures. Depending on the management style within the organisation, leaders might also have to spend a certain amount of time feeding their own beast.

In spite of these conflicting demands, the above tips for good portfolio management have a single common theme: they're about the teams, and the importance of enabling and supporting teams to deliver their best work.

This is because the portfolio office is uniquely positioned to set the organisation's tone and culture by creating the best environment for teams to thrive - and therefore to deliver value to users.

For leaders, this is the key takeaway: those thriving teams are the "adaptability muscle" in practice. Shifting the function of the portfolio office from one of policing to one of enabling is precisely how you build that muscle.

Designing for resilience

How to make readiness and recovery a core capability.

> Organisations that embrace disruption as an opportunity, rather than a threat, will be the ones that thrive in an era of continuous change.

The resilience muscle: how to endure shocks and emerge stronger

Rob Miller

In business today, there are two types of organisations: those that are resilient, and those that will not survive the next major shock. This isn't hyperbole - it's the new operational reality.

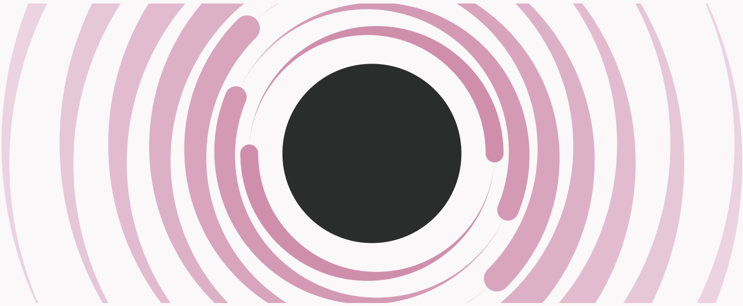
While adaptability allows an organisation to seize opportunities, resilience is the organisation's core capacity to withstand the inevitable shocks of a complex world, recover with speed and confidence, and emerge stronger. This is more than just a defensive strategy: it's a source of profound competitive advantage.

A crisis may come from a sophisticated cyber-attack, or a flawed software update. It could be a critical supplier failing overnight, a disruptive new technology upending your market, a sudden political shift, or a global pandemic that rewrites the rules of business.

Recent years offer a catalogue of such incidents: crippling cyber-attacks on Marks and Spencer and Jaguar Land Rover; supply chain breaches impacting the NHS; and the faulty CrowdStrike update that grounded flights and halted businesses worldwide.

For a leader, the specific source of the crisis matters far less than the organisation's practiced, ingrained ability to respond.

> The greatest barrier to building true resilience is a leadership mindset that treats failure as a possibility to be prevented, rather than a certainty to be prepared for.



The critical mindset shift: plan for 'when', not 'if'

The greatest barrier to building true resilience is a leadership mindset that treats failure as a possibility to be prevented, rather than a certainty to be prepared for.

The only safe bet is to assume your controls will eventually fail. Every business today is a digital business, and in a deeply interconnected and fragile technology ecosystem, something will eventually break.

This means that the real work is not in achieving an impossible state of 'safety', or perfect security, but in the continuous practice of becoming 'safer'.

This requires a fundamental shift in focus: from prevention alone to a deliberate balance of preparation, response and recovery. The most important question is not "Have we prevented all bad things from happening?" but: "When a bad thing happens, how quickly can we recover, and what will we learn from it?"

This is not to say that organisations should stop trying to protect themselves against threats, but that they cannot rely on defences alone. It is equally as important to proactively invest to systematically reduce risk, and test the measures required to continue to function if the worst does happen.

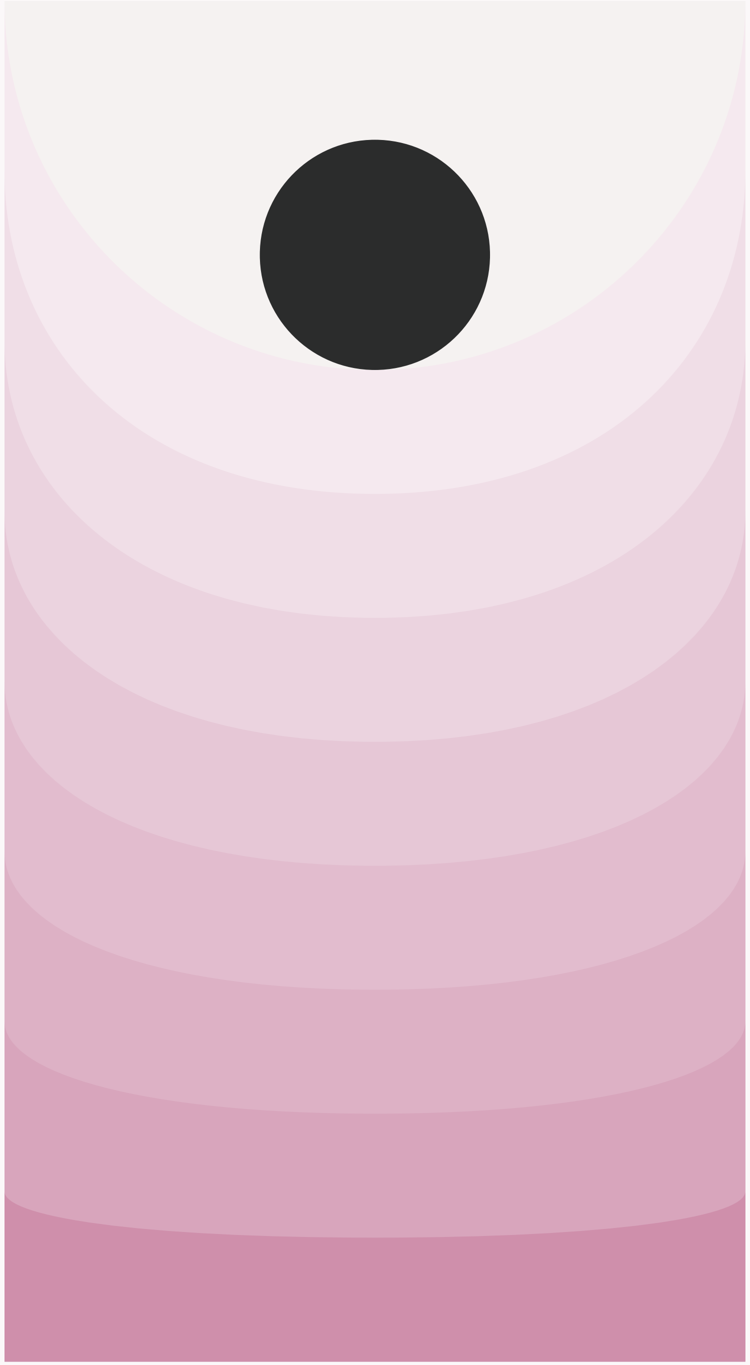
This shift moves resilience from the domain of technical insurance policies to a central pillar of strategic leadership, as fundamental to the organisation's survival as the oversight of its financial health or legal integrity. It acknowledges that while you cannot control the storm, you can build a ship that is designed to weather it.

Resilience is built, not bought

Like any muscle, resilience is built through consistent, intentional practice. This muscle isn't strengthened by writing contingency plans that sit on a shelf, but through deliberately and safely testing your organisation's responses *before* a real crisis hits.

It cannot be outsourced or purchased as a technology solution. In fact, we would argue that attempting to outsource risk is more likely to increase the level of risk you are exposed to.

Resilience is an organisational capability that grows directly from the cultural conditions that leaders create. Building it requires confronting the "leadership-debt" of past decisions: the outdated processes, rigid hierarchies, legacy technology and cultures of blame and siloed working that prevent teams from responding effectively when failure strikes.



> A resilient organisation treats failures and near-misses as its most valuable sources of intelligence.

Countless organisations - including those who believed their risks were well managed - have become victims of devastating disruption. But others, like digital bank Monzo, have taken a different, more proactive approach. In planning for catastrophic failure - a complete outage of their cloud provider - they've built a standalone 'stand-in service'.[1] This is a separate, simplified system designed for the sole purpose of keeping card payments working if the main platform goes offline. Crucially, they've used this service, for real, on more than one occasion.

This isn't just a disaster recovery plan, it's resilience that is engineered by design - a tangible investment in ensuring their most critical services remain available, no matter what.

This commitment proves a critical point: resilience doesn't come from compliance certificates or ticking boxes. It is built on two core principles, which must be established and championed by leaders:

1. Empowered, multi-disciplinary teams. In a crisis, the instinct for centralised, top-down control is strong, but it's too slow to be effective. Resilience depends on empowered teams who have the autonomy, context and authority to solve problems at the front line.

2. A culture of learning, not blame. A resilient organisation treats failures and near-misses as its most valuable sources of intelligence. This requires absolute psychological safety - an environment where people can flag vulnerabilities and admit mistakes without fear of punishment. When blame is the default response, problems are hidden, lessons are lost, and the organisation becomes progressively more brittle. When learning is the goal, every incident becomes an investment in future strength.

[1] pdlink.co/monzo-standin

Putting resilience into practice

Building resilience is an act of leadership. It requires deliberate actions that make the principles of empowered teams and a learning culture a reality. For leaders, the work is not to become a technical expert, but to lead the application of these three practices:

These three practices - mapping, testing and drilling - reinforce a single, vital lesson for leaders: crisis response and preparedness is a team sport. It cannot be delegated solely to the IT department, but is an organisational capability built on the connections and shared understanding between teams across the entire business.

1

Map what matters most

A leader cannot defend what they don't understand. Ensure the organisation has a clear and current understanding of how it delivers value. Building a complete and accurate map of critical services requires empowered, multidisciplinary teams - experts from technology, operations and customer-facing roles - who can create a shared picture of what matters most.

2

Stress-test your reality

Simulate disruption to your organisation's infrastructure to stress-test your assumptions. This exercise is not about creating fear - it's about exposing blind spots before a real crisis does it for you. This is only possible if teams feel courageous enough to ask uncomfortable questions and expose the organisation's fragile points.

3

Normalise the 'fire drill'

Building resilience must go further than testing whether computers can be restarted, and should include testing how you will continue to function if they can't. The leader's role is to normalise the act of practicing for failure, transforming it from a dreaded audit into a routine and productive "fire drill". This cultural shift makes it safe for empowered teams to practice their crisis response and find weaknesses, with the shared understanding that every flaw discovered in a drill is a crisis averted in the real world.

The competitive advantage of bouncing back

While it may seem like a defensive investment, a well-developed resilience muscle delivers a powerful competitive edge. When a systemic shock hits, the human impacts are real and severe, leading to scenarios where thousands of hospital operations are cancelled, suppliers face bankruptcy, jobs are put at risk.

In these moments, the organisations that survive and thrive are those that can get back on their feet the fastest. While unprepared competitors are paralysed by indecision or crippled by outages, the resilient organisation is already executing its recovery playbook, focused on restoring critical outcomes for its customers, maintaining their trust, and capturing market share while competitors struggle simply to get back online.

This confidence in the ability to recover also allows an organisation to take smarter risks. It can embrace new opportunities, including new technologies, knowing that if an experiment fails, it has the strength to absorb the impact and use the valuable learning to inform its next move. Resilience, in this sense, is the stable platform from which an organisation can confidently leap.

Building resilience is a duty of care

Let there be no ambiguity: a major incident is a question of ‘when,’ not ‘if’. For too long, this reality has been treated as a technical problem to be delegated and validated through periodic certifications. It is not. Building resilience is a fundamental and vital duty of leadership, and must be treated with the same gravity as financial stewardship or legal compliance.

As such, the crucial question is not *if* you should build resilience, but *how* you create the conditions for it to grow. In an era where a single point of failure can threaten the entire enterprise, the culture you foster is the ultimate measure of your organisation’s fitness to survive.

A playbook for navigating a crisis

Matthew Sheret

When a major incident strikes, the pressure on leadership is immense. The natural instinct is to lock down, centralise, and control every decision. But this is the moment that reveals the true strength of your organisation. A crisis is the ultimate stress test of your resilience muscle; the preparation you do beforehand is the training, and the incident itself is the moment of truth.

This is the playbook for when the fire alarm is real.

The fastest path to recovery lies not in top-down control, but in using the same tools and habits that build a modern, adaptive organisation. It's about applying core practices like service mapping, outcome-driven development, empowered teams and transparency to the critical challenge of recovery.

This guide provides a playbook for leaders to do just that, helping you navigate the crisis and get your organisation back on its feet, fast.

1. Map what your organisation does

It's absolutely fundamental that you have a high-level understanding of what your organisation does. It seems like a facile thing to say, but in large organisations there can be huge areas that are relatively opaque to central operations teams.

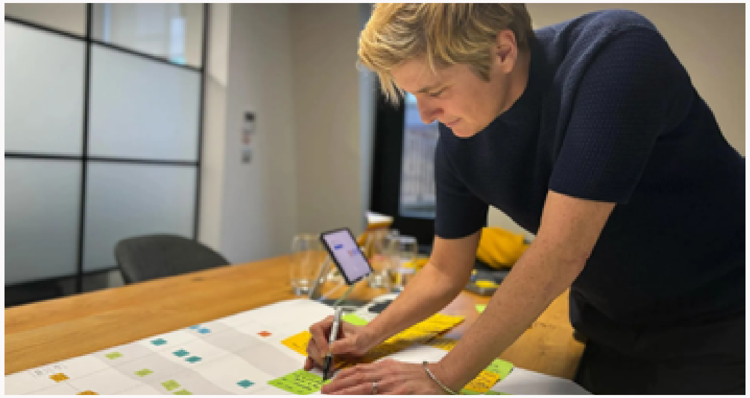
This service map doesn't need to be at the task-by-task level. But it should illustrate the journey your customers and/or internal teams go on. It will be an essential asset for recovery planning.

What this map needs to include will be different for different organisations. For news outlets, how do stories flow from source to screen? For retailers, what are the steps that take you from thinking to trading? How do you pay staff and suppliers?

Getting together a cross-functional team will help you make a comprehensive map. At the same time, a neutral facilitator will ensure people don't get lost in the details. Both of these are important foundations for the actual work of recovery too (more on that below).

As you build these maps, you'll see the flow of information through your organisation. Pinpoint your priorities: what's essential? It'll take time to recover your systems: what activities do you need to find workarounds for right now?

The best time to make this map is now (i.e. before an incident has occurred). Having this in your back pocket can save hours, or even days. If it's too late for that, then get a team working on this while others focus on securing your systems.



Service mapping is an essential asset for recovery planning.

2. Highlight the capabilities you have, and the ones you don't

Use your map to work out what you've lost.

In many organisations, the systems your teams use are likely to be highly fragmented. Those silos might be helpful: you might be frozen out of your CRM, but have complete access to your inventory tools. In other words, your gaps will be partial. But it might be that the critical systems that underpin several parts of your operation are effectively gone.

Come back to the priorities on your map: what can you actually do now? Your team (and your suppliers) must be clear about which systems you can trust, and what data is accessible.

You'll likely find yourself with a map that shows things like:

- We can file draft copy for review, but we can't publish it
- We can design new products, we cannot send these to suppliers
- We can track inventory on existing third-party systems, but cannot connect it to our central database

Whatever the specifics, your map will show you where the gaps are. Use this to understand which gaps are most critical and prioritise these.

It's worth noting that this map of what's possible (and what's missing) will fluctuate. You'll learn by the hour whether "safe" systems have actually been compromised, or whether you have access to unaffected third party systems. That's normal.

3. Focus recovery efforts around outcomes

You should now understand:

- What the most important needs are to your organisation
- Which of these you can't currently meet
- What to fix first

With a system-wide outage, the temptation will be to solve every problem at once. Outcomes keep teams on track.

Get started with a clear outcome. Something like "We can communicate with customers who have placed orders with us."

Those outcomes will help you work out who needs to be in your recovery teams. Make sure there's a voice for the end user on board too (whether it's your customers or your colleagues), as well as delivery and facilitation support. These skills will help your team stay honest about the outcome they're working towards.

> in times of crisis the traditional response is to lock down, close up, stay guarded. That approach won't lead to quick recovery.

4. Empower teams to plug the gaps

Empowered teams need to be able to create solutions, not just think about them. As well as making sure the team has a blend of technical, operational and specialist skills, they need a mandate to deliver on their outcome. That means:

- Permission to test and learn
- Access to users (whether those are colleagues or customers)
- Authority to talk to partners and suppliers
- Visibility of the work of other teams
- A route to escalate problems that are blocking progress

This list shouldn't come as a huge surprise - it's baked into the advice we give to all our clients. But in times of crisis the traditional response is to lock down, close up, stay guarded. That approach won't lead to quick recovery. Yes, it's important to be disciplined about what a recovery team deploys. But the near-term view needs to pair security with recovery.

Be mindful about how sustainable this work is. As my colleague Cate McLaurin writes in her piece on leading through a crisis: "The intense pressure of crisis management can lead to burnout."[1]

As days roll into weeks, consider rotating some of the experts in these teams. Partly, this will give people a breather. But you'll also be distributing knowledge about what's going on. This will be especially important once the workarounds are in place and these teams start maintaining the solutions they've built.

[1] http://pdlink.co/leading-through-cyber

5. Be open about progress

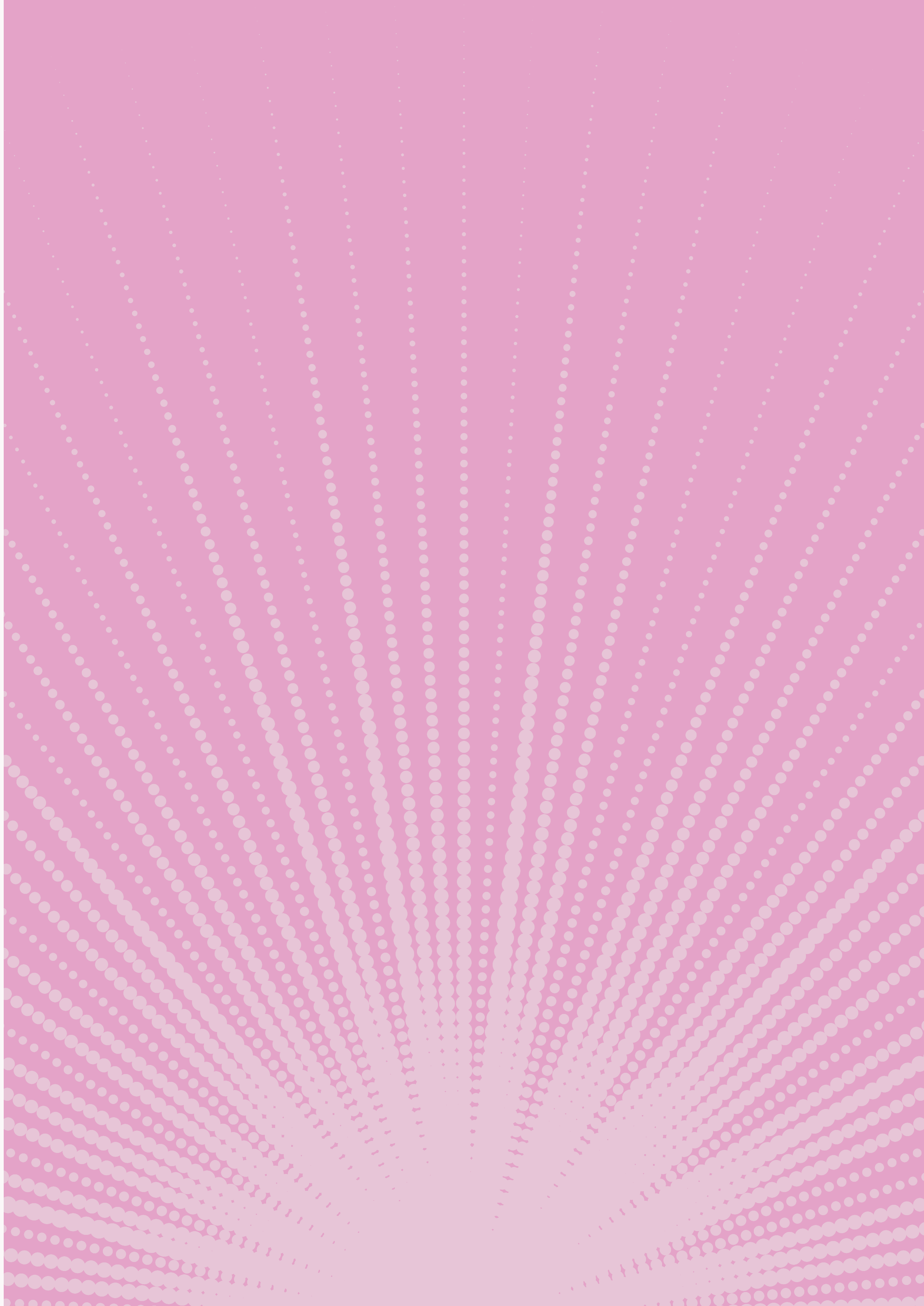
Successful recovery demands tight-knit communication. It's likely you'll have multiple teams trying to stand up different processes. Clear outcomes should mean teams aren't stepping on one another's toes. But there may still be times when those teams need support from one another, or are competing for people and data.

In the first few days of recovery, get the leads and/or facilitators to check in a couple of times a day. Ideally, these will be light-touch updates so leaders and colleagues can learn: here's where we're at, here's what's blocking us, here's what we need. This isn't a time for leaders to get stuck into the minutia of the work. It's about visibility, and clearing a path for your recovery teams to deliver.

Create time for other teams to ask questions: "Are you capturing the data I need? Are you looking at how to connect our services?".

This should also be when you share updates about what data and tools are (or aren't) available. Any change is likely to affect the scope of one (or all) of the teams developing workarounds.

While this work is going on, keep the wider organisation in the loop. Manage these updates centrally: don't put the weight on your recovery teams until they're sharing tutorials or managing feedback. Remember, trust will be low. Without this heartbeat, it'll evaporate entirely.



> At Public Digital we say that a major incident is a question of 'when,' not 'if.

Start preparing now

Depending on the extent to which your systems have been compromised, the road to recovery might be long. The journey isn't going to be linear: progress will come in fits and starts.

At Public Digital we say that a major incident is a question of 'when,' not 'if.' Whether caused by a malicious attack or an internal failure, critical systems will eventually break. The best way to embolden your response - and pick your organisation up faster when you are knocked down - is to start preparing now.

Build your maps. Understand how you operate, truthfully. Grow your confidence in using cross-functional teams, and outcome-driven approaches.

The work of preparing for a crisis is indistinguishable from the work of building a modern, adaptive, and resilient organisation. They are one and the same.

Using chaos-testing to build like it's already broken

Linda Essen-Möller

Before transformation, there is often disruption. Before innovation, there is usually a crisis that forces organisations to change. When things go wrong - whether through systemic failure, an external attack or sudden market shifts - organisations are forced to re-examine their ways of working. This isn't merely about fixing what's broken: it's about adapting to ensure the same mistakes aren't repeated.

Chaos testing is the term used to describe the process of software engineering that deliberately introduces failures into a system to test its resilience. Companies like Netflix pioneered the concept with tools like Chaos Monkey, which randomly disrupts infrastructure to expose vulnerabilities. However, the same principles can apply to whole organisational design - and not just to resilience.

Think of chaos testing as your organisation's fire drill. It is a planned, controlled practice designed to build muscle memory and expose weaknesses in your response before you have to deal with a real fire.

For example, a company can test the strength of their strategy by asking: What would happen if their largest customer suddenly walked away? They can also assess the stability of their leadership by evaluating how the business would fare if key senior team members were to leave. Moreover, it's vital to test a company's ethical framework by considering the potential reputational risks associated with emerging technologies such as AI, and asking: could the ineffective implementation of an AI system - such as failing to upskill workers - lead to significant damage to the company's reputation? Chaos testing allows businesses to identify vulnerabilities, improve risk management and enhance their ability to adapt in the face of uncertainty.

True organisational chaos testing isn't just about infrastructure - it's cultural. It asks uncomfortable questions. What if your leadership team was publicly compromised? What if your product went viral for the wrong reason? What if your AI tools discriminated without you knowing? How reliant is the data we use to inform decisions? How quickly are we able to respond to change?

These questions aren't hypothetical - they are real scenarios which play out across industries. To answer them, and to run meaningful tests, leaders must begin with the foundational work of service mapping: creating a clear picture of what your organisation actually does and the critical systems it relies on. The best-prepared organisations are those that simulate disruption, forcing themselves to respond to worst-case scenarios before they occur in reality.

In an age of AI hallucinations, deepfakes and climate-induced migration, the real risk is assuming that business-as-usual will carry you through.

Why crisis is a catalyst

As Public Digital's founders write in their book Digital Transformation at Scale, most organisations do not change unless they have to.[1] In the commercial sector, existential threats demand action: delays risk the loss of customers, revenue or relevance. In government, where institutions can often weather crises without immediate existential risk, inertia is a greater challenge. Yet, as the digital era reshapes services and expectations, even the public sector must acknowledge that 'the way we've always done things' is no longer good enough.

Some crises stem from technology failures, such as when Canada's payroll system left 80,000 employees underpaid or the NHS faced a ransomware attack that resulted in a blood shortage. Others result from policy implementation breakdowns, like The Post Office scandal or Centrelink's controversial debt recovery programme in Australia. And in the corporate world, even household names have crumbled under complacency - Nokia, Thomas Cook, Debenhams, Woolworths and HMV serve as cautionary tales of failing to embrace digital change in time. Barclays, Tesco and Aviva, meanwhile, show how other companies got it right.

[1] http://pdlink.co/dts

Breaking the cycle of complacency

Crises reveal the flaws in existing processes, but the response determines whether an organisation learns and improves. Too often, organisations patch the immediate problem and move on, rather than addressing the underlying structural weaknesses. This is particularly true in government, where the pressures of day-to-day firefighting can make long-term reform seem unattainable.

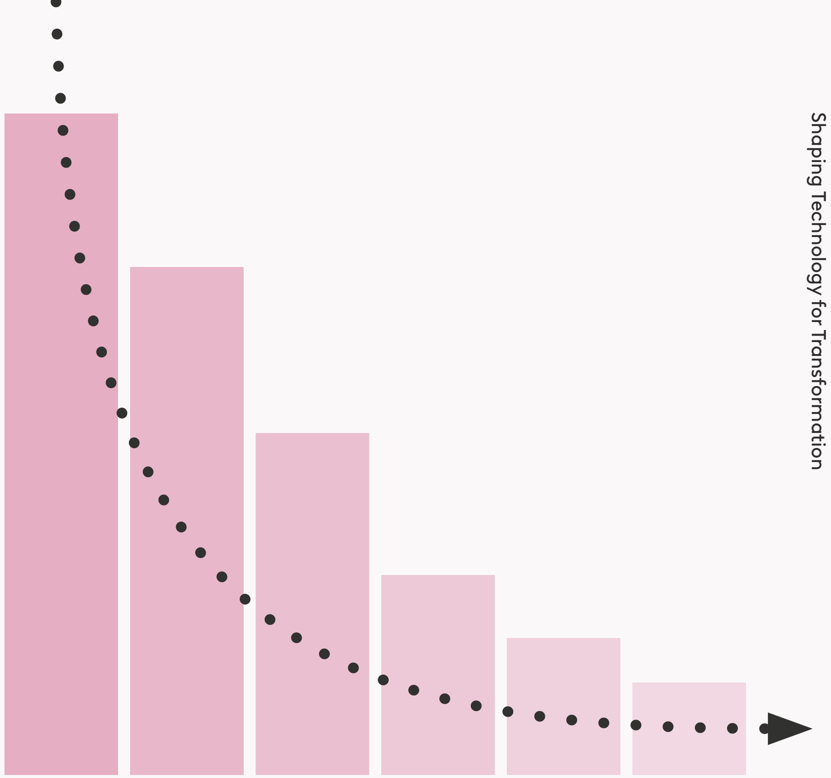
As Greenway writes, In the commercial world, crises tend to focus the mind because they can be genuinely existential: "Fail to respond, and all of a sudden your company name is no more than the punchline to a bad joke. Sony's reluctance to develop a competent digital Walkman left space for Apple's iPod. Video rental giant Blockbuster airily dismissed Netflix, then went bankrupt when it couldn't compete. Many companies don't heed the call - often those that have become so big they can't imagine a world without them in it. All too often, the rest of the world has no such difficulties."

Companies tend to be most at risk when they are enjoying comfortable profitability, Greenway reminds us. With good profits and a rosy outlook, the need for dramatic change is obscured. This sort of complacency is only ever justifiable if your organisation doesn't use technology and is immune to fundamental social changes - a state which is exceedingly rare today.

Real transformation happens when leaders seize moments of disruption as opportunities to implement lasting change. This means:

- Investing in resilience - ensuring digital systems are flexible, modular and built to withstand disruption.
- Encouraging experimentation - creating safe spaces for testing new approaches and behaviours, even if they challenge traditional norms.
- Learning from failure - embedding a culture that analyses missteps constructively, rather than defensively.
- Allowing time to transform - embedding new ways of working doesn't happen overnight; employees need space and time to change their habits and behaviours.

Whether it’s adapting to remote work overnight during a pandemic or rapidly deploying digital services when legacy systems fail, necessity drives action.



A crisis is too good to waste

As history shows, crises force organisations to move faster than they ever thought possible. Whether it’s adapting to remote work overnight during a pandemic or rapidly deploying digital services when legacy systems fail, necessity drives action. The challenge is to ensure these moments don’t result in short-term fixes but lead to long-term change.

Chaos testing is not about inviting failure - it’s about preparing for the inevitable. Organisations that embrace disruption as an opportunity, rather than a threat, will be the ones that thrive in an era of continuous change.

Conclusion: The foundations of meaningful change

Dai Vaughan

This collection of articles has taken you on a journey. It started by diagnosing your **foundations** - how the "digital geology" of your history and the "leadership debt" of your culture affect how you operate today. It then showed you how to build the proactive **muscle of adaptability** to navigate constant change, and the defensive **muscle of resilience** to withstand inevitable shocks.

This book, while ostensibly about technology, is not really about the technology itself. It's about the culture, mindset and leadership conditions that allow technology to be effective.

Technology does not transform an organisation. The code, the cloud infrastructure, and the AI tooling are not transformative by themselves. Instead, their impact depends on whether the organisation has first built the foundations for change - developing a deep understanding of their customers, adopting a test and learn mindset, and building a culture of empowered teams. These are the ways of working explored in this series of books.

Building those foundations requires firstly the It means having the humility to admit you don't have all the answers about what your customers truly need, and secondly the commitment to work in the open to discover those answers. It means shifting your focus from delivering outputs to achieving outcomes. These are not just processes; they are the daily acts that build the trust and transparency at the heart of an adaptable and resilient organisation.

This requires a fundamental shift in your operating model, moving from siloed functions to empowered, multidisciplinary teams - which form the fundamental unit of delivery for both adaptability and resilience. They are the teams who can build, test, and learn at the speed required by the AI era, and they are the teams you will depend on to execute a crisis playbook when a real incident strikes.

This shift in structure is impossible without a shift in leadership. It requires reframing leadership's role: moving from a function of control and reporting to a service that provides teams with context, removes blockers, and builds the "guardrails" that allow for safe experimentation.

For leaders, the message from this is clear: technology is a core leadership responsibility, not a function to be delegated or outsourced. Your primary role is to build these teams and create the conditions for them to win. Ultimately, you must prepare for both change and failure; your organisation's fitness depends on its capacity for both adaptability and resilience.

The good news is that none of us are alone in this. The chapters in this book reflect our experiences as leaders and working with organisations who have been on this journey. It's on you to make change happen in your organisation, but there are years of learning you can draw on to achieve that.

Throughout this book, we have framed technological strength as a "muscle". This metaphor is deliberate. You cannot buy it; you must build it, repetition by repetition.

These muscles are not built in the server room. They are built in the boardroom, in your team charters, and in your budget cycles.

Developing these muscles means that any other strategy work you do can be meaningful - and gives you the chance to deliver change successfully. But they aren't sufficient in themselves - as a leader you need to identify and set the strategic direction as well.

Achieving meaningful change starts with the foundations you build. The work of building them must begin now.

Questions for leaders to ask of their organisation

1 If we identified a critical new customer need today, how long would it take us to ship a working prototype to real users?

2 Where is our internal governance currently stopping teams from doing their best work?

3 Do we have the internal capability to change our technology strategy, or are we locked into our current path by our vendors?

4 When was the last time we deliberately broke something to test our ability to recover?

5 Can you show me a current map of our most critical services and the risks that sit beneath them?

Dai Vaughan
CTO, Consulting Practice

Dai is Public Digital's Consulting Chief Technology Officer and a non-executive director in the NHS in Wales. He has worked with clients including the Phoenix Group, HSBC, Heidelberg Materials and global governments in the US, Canada and the Caribbean. Prior to joining Public Digital, Dai was one of the founders of the Government Digital Service, where, as Head of Technology, he led the technology teams responsible for delivering the GOV.UK website.

Dave Rogers
Partner

Dave is a Partner at Public Digital. He leads our work in the UK public sector, and has advised clients including BT Group, Arup, the Home Office and UK Parliament, as well as international governments. Prior to joining Public Digital, Dave helped found the UK Ministry of Justice Digital team, and served as its Chief Technology Officer. He was previously a senior technical architect at the BBC.

James Stewart
Partner and CTO

James is a Partner and Chief Technology Officer at Public Digital, where he is a trusted advisor to clients including global governments, major non-profit organisations and international institutions like the International Monetary Fund, World Bank and UN agencies. Prior to joining Public Digital, James was Deputy Chief Technology Officer of the UK Government and was heavily involved in the formation of the UK's National Cyber Security Centre.

Julia Harrison
Senior Director

Julia is a Senior Director at Public Digital, where she has worked with clients including Canada's British Columbia Energy Regulator, the UK Department for Business and Trade, the Local Government Association, and the Stroke Association. She has over 10 years' experience working with and leading agile product teams across a range of organisations including Morgan Stanley, eBay, the Government Digital Service and HMRC.

Linda Essen-Möller

Senior Director

Linda is a Senior Director at Public Digital, and has been instrumental in growing Public Digital's commercial offer. She led our engagement with BT Group, driving programmes to enhance ways of working. Before joining Public Digital, Linda held senior roles at strategic innovation and technology company, Nortal, including Global Consulting Director and Head of Consulting in the Middle East.

Matt Harrington

Director

Matt is a Director at Public Digital and an expert product manager. He has worked with clients including BT Group, NHS England, the Premier League and the British Columbia civil service. Prior to joining Public Digital, Matt led product development teams at accuRx, a healthcare start-up now used by 99% of GPs in England, building services and mapping the path to growth.

Matthew Sheret

Director

Matthew is a Director at Public Digital, where he has supported our engagements with core commercial clients including M&S and HSBC. Matthew brings rich experience as a writer and strategist, having led a team building AI-enhanced legal services at Juno, and developed data-driven storytelling and new services at Last.fm. He co-wrote the first standard for digital public services at the UK's Government Digital Service.

Oli Lovell

Principal Consultant

Oli is a Principal Consultant at Public Digital, and has worked with clients including Change Grow Live, the University of Exeter, the Dutch Government, Arts Council and NHS Providers. Prior to joining Public Digital, Oli held senior leadership roles at the Met Office and at GCHQ, where he served as Lead Product Manager and Senior Service Owner for a complex data value stream supporting the UK's intelligence and cyber defence.

Rob Miller

Senior Director

Rob is a Senior Director at Public Digital, where he has supported purpose-led organisations including the Department for Environment, Food and Rural Affairs (DEFRA), Change Grow Live, and Southern Housing. He led our work with the Local Government Association to develop a cyber 'Grab Bag' for local authorities. Rob's prior experience includes strategic leadership and transformation across large, complex councils, most recently Hackney Council in London.

public·digital

Public Digital is a consultancy that works with large businesses, governments and institutions that matter.

We help them change their ways of working to become more responsive, adaptable and impactful.

This publication is the final edition in a three part series.

We welcome comments and feedback about
Shaping Technology for Transformation, or anything else.
Please get in touch by sending an email to contact@public.digital.

Scan here to work with us

Edited and published by
Public Digital

www.public.digital

Printed by

Generation Press