PROBLEM? RELAX. YOU'VE GOT THIS!

The Internet Vanished for a Week, and My Company Went with It

How to Identify Your Company's Dependencies on Internet Access and Cloud Services, Prepare Alternative Ways of Working, and Establish Customer Communication Without Improvising a Continuity Plan After an Outage



Max Paradox

The Internet Vanished for a Week, and My Company Went with It

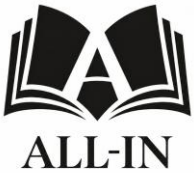
How to Identify Your Company's Dependencies on Internet Access and Cloud Services, Prepare Alternative Ways of Working, and Establish Customer Communication Without Improvising a Continuity Plan After an Outage

Max Paradox

PROBLEM? RELAX. YOU'VE GOT THIS!

ISBN: 9788384839126

ALL-IN Rafał Płonkowski



CONTENTS

INTRO 5

Chapter 1 - Your Business Is Hanging by an Invisible Cable..... 10

Chapter 2 - The Map That Reveals What Your Business Depends On 18

Chapter 3 - Two Internet Connections, Zero Working Orders..... 27

Chapter 4 - Everybody Has a Solution. Unfortunately, They're Different Solutions..... 36

Chapter 5 - The Emergency Procedure Nobody Knows How to Activate 45

Chapter 6 - Your Data Is Safe. Unfortunately, Nobody Knows Which Version Is Correct..... 53

Chapter 7 - When the Company Chat Goes Silent, Rumors Take Over 62

Chapter 8 - Your Provider Is Investigating. Your Customers Are Still Waiting..... 71

Chapter 9 - When Everything Is Urgent, Nothing Has Priority..... 79

Chapter 10 - Paper Doesn't Make a Process: Building a Workable Offline Workflow 87

Chapter 11 - Customers Don't Need Your Technical Diagnosis. They Need an Answer. 96

Chapter 12 - Seven Days Without the Cloud: Managing a Business That Cannot Simply Wait..... 105

Chapter 13 - A Business Continuity Plan That Doesn't Need Its Own Instruction Manual..... 116

Chapter 14 - Rehearsing a Disaster Without Causing One 125

Chapter 15 - What If It Isn't an Outage? When Getting Back Online Could Make Things Worse 135

Chapter 16 - When the Backup Plan Breaks and the Disaster Brings a Friend 144

Chapter 17 - The Exit Door Is in the Cloud Too 154

Chapter 18 - The Plan Was Ready. Then the Business Changed. 162

Chapter 19 - The Internet Is Back. Now Find Out What the Outage Really Cost. 171

Chapter 20 - A Company That Can Carry On Without Waiting for a Miracle 179

INTRO

At 10:12 on a Wednesday morning, a delivery driver is standing outside a garden supply company, waiting for someone to tell him where to unload four hundred young trees. The warehouse manager knows the shipment is expected. Unfortunately, the delivery schedule lives in a cloud application that has stopped responding. The purchasing department cannot open the supplier's order confirmation. Customer service cannot check which trees have already been sold. Meanwhile, the driver is considering whether the company intends to pay him for the privilege of becoming a temporary outdoor storage facility. Outside, the trees are enjoying the sunshine. Inside, twelve employees are discovering that a business can possess buildings, inventory, vehicles, and perfectly functional human beings while being unable to answer a remarkably simple question: where does this delivery belong?

Someone suggests restarting the computers. Someone else calls the internet provider, who cheerfully confirms that the connection is working. The IT contractor reports that the cloud platform appears to be experiencing difficulties. Management requests an estimated restoration time, which produces the internationally recognized technical diagnosis, "We're investigating." For the first hour, everyone assumes normal service will return shortly. By lunchtime, customers are asking about orders. By midafternoon, employees have begun constructing improvised spreadsheets, each containing a slightly different version of reality. The warehouse manager finally asks whether anyone knows how to operate without the software. The room becomes quiet enough to hear the delivery driver checking the time.

Now remove the comforting assumption that the platform will return tomorrow. Imagine the disruption lasts an entire week. Your

company still has employees to manage, suppliers to coordinate, customers to serve, and bills to pay. The obligations haven't disappeared. Only some of the tools used to fulfill them have. That is the uncomfortable reality behind the title of this book. The internet does not need to vanish from the entire planet to create a serious business interruption. One unavailable cloud service, authentication provider, payment gateway, or network connection can be enough to interrupt operations that previously seemed effortless.

Modern businesses have good reasons to rely on connected technology. Cloud applications eliminate infrastructure headaches, automate repetitive tasks, and allow employees to collaborate across locations. Online ordering systems make transactions convenient. Shared databases keep information consistent. These improvements are valuable, and abandoning them would rarely be sensible. The problem begins when convenience quietly becomes dependence without anyone examining the consequences. A process that once required a telephone conversation, a document, and a decision may now require six digital services to cooperate successfully. Five can work perfectly while the sixth prevents the entire process from finishing. Unfortunately, business operations do not award partial credit because the authentication server performed beautifully while the order system was unavailable.

This is why the usual question, "Do we have backup internet?" is nowhere near sufficient. A second connection may protect you against a failure of the first one. It cannot repair a cloud platform that is unavailable to everyone. A backup file may preserve valuable information without providing the application needed to use it. A spare laptop accomplishes little if the employee cannot sign in. Even an excellent technology supplier may be unable to restore service as quickly as your customers need. Business continuity requires understanding the relationship between technical failures and business consequences. Otherwise, you can

spend a considerable amount of money protecting the wrong things, then discover during an outage that your beautifully redundant equipment is performing an exceptionally reliable version of nothing useful.

The distinction matters because not every interrupted activity deserves the same response. Some tasks can safely wait. Others must continue within a limited time to avoid serious losses, contractual problems, or safety risks. Certain operations should actually stop when trustworthy information becomes unavailable. Processing transactions against outdated records, for example, may create duplicate orders or incorrect commitments that take longer to repair than the original outage. A sensible contingency arrangement therefore involves deliberate compromises. It may preserve essential services while temporarily suspending less important activities. That is not failure. It is the difference between controlling a difficult situation and pretending that the company remains capable of everything it could do yesterday.

People are central to this equation. A written procedure has limited value if nobody knows when to activate it, who is authorized to make decisions, or where to find it when the usual systems disappear. Employees also have practical constraints. They become tired, work different shifts, take vacations, and occasionally have reasonable objections to being designated the emergency solution to every organizational problem. A business that relies on one exceptionally knowledgeable employee is exposed when that employee is unavailable. Nor can a manager simply announce that everyone will work twice as hard for a week. Human beings are not software subscriptions with an unlimited-capacity upgrade.

Customers introduce another complication: they experience your disruption through its effect on their own lives. They rarely care which technical component failed. They care whether their order was accepted, whether a scheduled service will happen, whether their payment is secure, and when they will receive useful

information. Silence invites speculation, while confident promises based on guesses create additional obligations. Good communication does not require knowing the exact restoration time. It requires distinguishing confirmed facts from assumptions, explaining the consequences honestly, and establishing when further updates will be provided. Customers may dislike delays, but discovering that three representatives have promised three incompatible outcomes tends to make the experience considerably worse.

This book will help you examine the operations that keep your company functioning, identify their hidden dependencies, and decide what genuinely needs protection. You will learn how to distinguish a technical problem from its operational effects, prepare workable alternatives, and recognize when continuing a process would introduce unacceptable risks. We'll also explore how to cooperate with technology providers, protect essential information, organize communication, and test contingency arrangements before they are needed. The objective is not to reproduce every capability of your normal systems at any cost. It is to maintain the most important business outcomes through methods that employees can understand, execute, and verify.

There are limits to what preparation can accomplish. A small business cannot necessarily afford duplicate infrastructure, a dedicated recovery facility, or several independent technology teams. Some disruptions will require specialist assistance, particularly when cybersecurity, sensitive information, legal obligations, or physical safety are involved. No sensible book can guarantee that every outage will be harmless. What you can do is reduce unnecessary uncertainty, make choices about acceptable interruptions, and establish reliable ways to respond when circumstances become less cooperative than the business plan anticipated.

Perhaps the most useful change will be in how you think about preparedness itself. It does not begin with purchasing another service or producing an impressive document. It begins by asking what would happen to a real customer request if your most important digital tools stopped working this afternoon. Which information would employees need? Which commitments could they safely honor? Who would authorize exceptions? What would they communicate if the outage lasted longer than expected? These questions are uncomfortable precisely because they reveal what a normal working day allows us to overlook.

The internet may eventually return without your intervention. Your business, however, needs to remain capable of making sensible decisions before that happens. And if the next outage arrives on a Wednesday with four hundred trees waiting outside, it would be rather nice to know where to put them without first negotiating with a cloud server.

Chapter 1 - Your Business Is Hanging by an Invisible Cable

The workshop had three industrial 3D printers, two laser cutters, a cabinet full of expensive materials, and a team capable of producing architectural models that made unfinished buildings look significantly more attractive than they would probably be in real life. Its owner had invested carefully in equipment and maintenance. Every important machine had been serviced, spare components were available, and employees knew how to handle common technical problems. Then, one Thursday morning, the software used to prepare production files refused to open. The computers worked. The machines worked. The internet connection worked. Unfortunately, the application needed to verify its license through an external service that was temporarily unavailable. Six perfectly functional machines stood idle because a computer somewhere else could not confirm that the company was allowed to use software it had already paid for.

The production manager initially treated the problem as a minor inconvenience. Someone suggested reinstalling the application, another employee checked the network, and a third investigated whether the company had accidentally forgotten to renew its subscription. After an hour, the team discovered that the licensing provider had acknowledged an outage but offered no reliable restoration estimate. The workshop could finish a few jobs using files prepared earlier, but new designs could not enter production through the normal process. Its expensive equipment had become a collection of unusually sophisticated furniture. Nobody had considered software licensing a critical production dependency because licensing was something that happened quietly in the background. Until that morning, the most interesting thing about the license had been its annual price.

This fictional workshop illustrates a weakness that appears in businesses of almost every size. Companies understand their visible resources reasonably well. They know which employees perform important tasks, what equipment they own, and which products they sell. Their understanding becomes less reliable when the discussion moves to the invisible services connecting those resources. An employee may know how to complete an order without knowing that the procedure requires an external identity provider, a cloud database, and an integration maintained by a contractor who left the project eighteen months ago. These dependencies are not necessarily signs of bad management. Many are the perfectly ordinary consequences of adopting useful technology. The danger comes from allowing them to remain undiscovered until something fails.

When a Useful Tool Becomes a Dependency

There is an important difference between using a service and being unable to operate without it. A company might use an online dashboard to examine sales trends. If the dashboard disappears, management temporarily loses a convenient analytical tool. The underlying sales activity may continue. Another business might depend on that same service to calculate prices, authorize orders, and release shipments. Its interruption would have immediate operational consequences. The technology could be identical while the business exposure is entirely different. That is why identifying important dependencies requires looking beyond the names of applications and examining what people actually need them to accomplish.

Dependencies also change over time. A scheduling platform may begin as an optional convenience for a team of four. Three years later, it could coordinate eighty employees, customer appointments, vehicle assignments, and automatic notifications. Nobody formally decided to make the entire business dependent on the platform. The dependency developed gradually as more

activities were connected to it. Because the system was reliable during normal operations, the expanding exposure attracted little attention. The company became more efficient while also becoming more vulnerable to a particular interruption. Both developments can be true at once, although technology sales presentations understandably tend to emphasize only the first.

An effective starting point is to follow the consequences of a failure rather than concentrating exclusively on its technical cause. Suppose a customer cannot complete an online purchase. That is a visible symptom. Perhaps the checkout application is unavailable, payment authorization is failing, or an authentication service prevents customers from accessing their accounts. Each possibility suggests a different technical response. From the business perspective, however, the immediate questions concern whether orders are being accepted, whether money may have been charged, and whether customers are receiving accurate confirmations. Understanding the operational impact allows managers to make appropriate decisions while technical specialists investigate the underlying problem.

It also prevents the company from treating every error message as a disaster. Some interruptions have little immediate effect. Others may create serious problems even when the affected system appears unimportant. Consider a small application that sends approved product specifications to a manufacturing partner. Employees use it for only a few minutes each day, yet without it production instructions cannot be released. A system's importance cannot be measured simply by how frequently somebody opens it. The meaningful question is what happens when the task it supports cannot be completed. A tiny service can occupy a surprisingly large place in the company's ability to keep its promises.

The Failure Behind the Failure

The phrase "the internet is down" covers an impressive variety of situations. The local connection may have failed, but the problem

could also involve internal networking equipment, DNS resolution, a cloud provider, authentication, a software integration, or access permissions. Sometimes the network is functioning perfectly and the application itself is unavailable. Sometimes the application loads but cannot retrieve the information required to complete a transaction. These distinctions matter because a solution suitable for one problem may accomplish nothing against another. Purchasing another broadband connection will not restore an unavailable cloud database, regardless of how reassuring the second router looks beside the first.

Partial failures are especially deceptive. An employee might enter an order successfully while the warehouse never receives it. The accounting system could generate an invoice even though the associated transaction has not been confirmed. A customer may receive an automated message indicating that a service has been completed when the operational system still considers it unfinished. Because individual applications remain accessible, employees may assume the overall process is functioning. Meanwhile, information begins to diverge between systems. The resulting mistakes can be more expensive to correct than an obvious interruption that forces everybody to stop.

A useful way to understand these incidents is to separate the failed component, the interrupted activity, and the business consequence. A licensing service becoming unavailable is a technical event. The architectural workshop's inability to prepare new production files is an operational interruption. Missing a customer's agreed delivery date, paying employees for idle time, or hiring an outside supplier are possible business consequences. These three levels belong together, but they should not be confused. A technician naturally focuses on restoring the component. A production manager needs to understand which jobs can proceed. The owner must assess the effect on customers and

commitments. Good decisions require the perspectives to meet without pretending they are interchangeable.

Time adds another dimension. A service that can disappear harmlessly for thirty minutes might become critical after an afternoon. Some work accumulates and can be completed later. Other work becomes impossible once a deadline passes. A postponed internal review may be inconvenient; a missed opportunity to submit an important customer proposal may be irreversible. That difference is why statements such as "we can survive a day without this system" should be examined carefully. Who established that limit? Does it apply during the busiest period? What happens to the backlog? An estimate based on a quiet Tuesday may be rather optimistic during the final hours before a major delivery.

Stop Counting Applications and Start Following Work

Businesses often begin assessing their technology exposure by asking the IT department for a list of systems. The resulting inventory can be useful for maintenance, licensing, and security. On its own, however, it rarely explains how work happens. Two departments might use separate applications that depend on the same login service. Another process might depend on an informal spreadsheet managed by one employee rather than on any officially recognized system. An application inventory tells you what the organization uses. Understanding business dependence requires knowing what each activity needs, when it needs it, and what happens when those requirements are unavailable.

The invisible human dependencies deserve particular attention. Some employees possess specialized knowledge that has never been documented. A purchasing coordinator may know which supplier accepts emergency orders by telephone. An operations assistant may understand how to resolve unusual customer records that the official procedure never mentions. Such knowledge can be valuable, but it becomes a vulnerability when nobody else can

perform the task. This does not mean distributing every administrative password or expecting everyone to acquire every skill. It means recognizing where access, authority, or knowledge is concentrated and deciding whether the business needs an authorized substitute.

External suppliers introduce further complications. Your company might depend on a service provider that relies on another provider for hosting, messaging, or identity management. You do not necessarily need a diagram of every subcontractor's infrastructure. You do need to understand the important boundaries of responsibility and which external failures could prevent your business from operating. Two software products with different branding may share an underlying service. Two offices may connect through a common network component. Redundancy that appears convincing on an invoice may be less convincing when the shared component fails. The number of subscriptions is not a recognized measure of resilience, despite the enthusiasm with which some companies collect them.

Information itself is another dependency. A file can exist without being accessible. Accessible information can be outdated or incomplete. Employees may have a copy of a customer order but lack the latest modification agreed through another channel. During an interruption, acting on uncertain information sometimes creates greater harm than delaying the task. The relevant question is not simply whether a copy exists, but whether it is sufficiently current, reliable, and appropriately protected for its intended purpose. Sensitive information also requires proper security and access controls. Turning every employee's personal laptop into an emergency repository may increase availability while introducing an entirely different collection of problems.

Discover What Would Actually Stop

You can begin understanding your own exposure without launching a major technical project. Choose one ordinary business

day and identify a handful of activities that directly support customers or essential obligations. For each activity, ask what information must be available, which systems are required, who makes decisions, and what the next person in the process receives. Then consider what would happen if one requirement disappeared for an hour, a day, or a week. The purpose is not to invent an elaborate disaster. It is to discover which apparently routine steps would become impossible and what the consequences would be.

Make the questions specific enough to produce useful answers. Instead of asking whether the sales department could work without its CRM, ask whether an employee could confirm an existing order without it. Rather than asking whether finance needs internet access, investigate whether an urgent supplier payment could be safely verified and authorized. A general answer such as "we would manage somehow" conceals too many different possibilities. A specific answer identifies the missing information, the person responsible, and the limit beyond which the task should not proceed. If nobody knows the answer, record the uncertainty rather than making a reassuring assumption.

Include the people who actually perform the work. Official process descriptions often miss small but essential activities, particularly where departments exchange information informally. An employee might reveal that a daily export must be completed before another team can start, or that an automated email contains the only reference linking two systems. Such discoveries are useful even when they reveal weaknesses. They also explain why purchasing additional technology without understanding operations can be wasteful. Sometimes the most valuable improvement is establishing a reliable way to obtain a particular piece of information, not installing another expensive platform.

There is no need to eliminate every dependency. Doing so would require abandoning many of the technologies that make modern businesses productive. The goal is to understand which

dependencies are acceptable, which need protection, and which require a deliberate way of limiting activity when circumstances change. A company may reasonably choose to suspend some administrative work during an outage while protecting time-sensitive customer commitments. Another may need stronger safeguards because interruption creates safety or regulatory consequences. These judgments depend on the actual business, not on a universal list of applications that every enterprise supposedly must duplicate.

The architectural workshop does not need to stop using sophisticated design software. It needs to understand the implications of losing access to that software and decide how much protection its commitments justify. Perhaps some approved production files can remain usable under an appropriately licensed and secure arrangement. Perhaps the company must negotiate realistic delivery contingencies or investigate supported alternatives. What matters is that these possibilities are examined before a deadline forces an improvised decision.

An invisible dependency is not automatically a defect. It becomes dangerous when its failure can interrupt something important and nobody realizes that relationship exists. Once the connection is understood, the company can make a deliberate choice about what to protect, what to tolerate, and what to stop. Until then, an impressive collection of people and machinery may remain one unsuccessful login away from an unexpectedly expensive coffee break.

Chapter 2 - The Map That Reveals What Your Business Depends On

A business process diagram can be a beautiful thing. Rectangles line up neatly, arrows point in sensible directions, and every department appears to cooperate with the precision of a professional orchestra. Then somebody asks what happens when the booking system becomes unavailable, and the diagram suddenly develops a mysterious blank space between "customer request" and "service delivered." The original designer explains that this part is automated. Unfortunately, automation is precisely the thing that has stopped working. The diagram may accurately describe the ideal process, but it has neglected a rather important detail: what actually makes each step possible.

Consider a fictional company that rents lighting equipment for concerts, corporate events, and private celebrations. Its employees are experienced, its inventory is well maintained, and its customers appreciate being able to book equipment online. Management believes the operation is straightforward. Customers request equipment, the team checks availability, the warehouse prepares the order, and a delivery crew takes everything to the venue. At the end of the event, the equipment returns, its condition is checked, and the customer receives an invoice. Described this way, the business sounds wonderfully uncomplicated. The difficulties emerge when we examine the information and decisions connecting those steps. An elegant workflow can conceal an astonishing number of dependencies, rather like a stage production whose audience never sees the technicians keeping everything upright.

The purpose of dependency mapping is to make those connections visible. A useful map shows how work moves from an initial request to a meaningful result, which resources each step

requires, and where an interruption could prevent the process from continuing. It does not have to illustrate every computer, network cable, or database. Nor should it simply reproduce the company's organizational chart. Departments tell you who reports to whom. Process dependencies reveal what must happen before somebody else can do their job. The distinction is important because customers rarely experience your organization one department at a time. They experience the combined result, including any gaps between the departments.

Begin With a Result, Not a Rectangle

For the lighting company, the first question is what outcome we want to examine. "Equipment rental" is a reasonable starting point, but it covers several activities with different requirements. We might narrow the analysis to fulfilling an already confirmed event booking. The process begins when a booking is approved and ends when the correct equipment reaches the venue with the necessary documentation. Choosing those boundaries prevents the exercise from expanding into every possible business activity. Billing, returns, and maintenance remain important, but they can be examined separately or included where they directly affect this particular outcome.

Now follow one representative booking through the business. The sales coordinator confirms the customer's requested equipment and delivery date. The inventory system checks availability, including items reserved for other events. A technical specialist verifies that the selected products meet the event requirements. The warehouse receives a preparation list and allocates specific equipment. The transport coordinator arranges delivery, and the receiving party confirms what arrived. Each step needs an input, produces an output, and involves someone or something capable of performing it. These details create the foundation of a useful map because they show the handoffs where information can disappear, become inconsistent, or arrive too late.