PYRÉNÉES CAPITAL

Suite 9091, Building 15, Road 3801,
Adliya 338, Kingdom of Bahrain

+973 38873800
@ basil@pyreneescapital.com
www.pyreneescapital.com
CR No. 139655-1

The cost of digital dependence

The machinery of modern life works wonderfully. Until it doesn't — and then we discover how connected everything really is.

TENTH ANNIVERSARY EDITION · 2016–2026

19 November 2026

For a few days in November, America appeared to be losing an argument with its computers.

Bank payments dawdled. Office software took an unscheduled holiday. Flights were delayed. Even the National Security Agency had to explain a network problem in public — not, one imagines, its favourite sort of publicity. It was an impressive collection of institutions to be having an unimpressive week. [1]

Were foreign hackers having a particularly good week? Had artificial intelligence become too clever for the machinery beneath it? Or were ordinary faults finding their way through a world that can no longer function without its computers? The incidents appear to have different causes. That does not make the question less interesting. It makes the answer less convenient.

We can now pay, travel, shop and run businesses without giving much thought to the technology underneath. Which is precisely how most of us like it. Nobody buys a railway ticket hoping for a guided tour of the signalling equipment. Yet an increasing share of everyday life depends on services we cannot see, repair or replace when they stop working.

A crowded list of suspects

America has no shortage of people interested in its networks. US intelligence identifies cyber threats from China, Russia, Iran and North Korea, along with criminals who prefer making money without the inconvenience of running a country. These are real threats. They are not evidence that one of those groups caused November's outages. A list of suspects, however impressive, is not a solved mystery. [2]

US officials found no evidence of a coordinated attack, according to their public statements. They may well be right. Microsoft's preliminary account points instead to a fault that had been lurking for months. When traffic and available capacity changed, the fault surfaced; attempts to recover spread the trouble further. No international conspiracy required. Modern systems can make quite enough mischief on their own. [1,2]

Some safeguards worked. The NSA said its mission-critical capabilities continued; during the separate aviation disruption, aircraft already airborne landed safely. That deserves recognition. The important question is not whether a computer blinked. It is whether the essential service survived. [1]

A week of headlines does not prove that everything is breaking more often. Uptime Institute's 2026 research found fewer outages per data-centre site over five years. That is not a verdict on the whole economy. But here is the catch: a rare failure can become a much bigger event when an extraordinary number of people depend on the same thing. [5]

PYRÉNÉES CAPITAL

Suite 9091, Building 15, Road 3801,
Adliya 338, Kingdom of Bahrain

+973 38873800
@ basil@pyreneescapital.com
www.pyreneescapital.com
CR No. 139655-1

“It’s life.” Is that the plan?

Asked about the disruptions, President Trump offered a wonderfully compact diagnosis: “It’s life.” “It’s fine,” he added. Big, rich and powerful countries do have problems. But wealth is not a backup system, and a customer waiting for wages to arrive might reasonably hope for something more useful than philosophy. [3]

The administration subsequently offered a fuller explanation and rejected the theory of a coordinated malicious attack. Intelligence director Jay Clayton called the rush to repair computer weaknesses a “good news story”. He has a point: finding a weakness is better than leaving it for criminals. The news is rather less cheerful when the repair interrupts the service. [2]

Washington’s initial response was breezy; the fuller official account was more useful. Either way, the public deserves to know which safeguards worked and what will be improved—not simply that the computers have been persuaded to behave again. [2,3]

When the cure becomes the problem

Senator Mark Warner has raised an intriguing possibility: AI may be finding weaknesses in software faster than the people responsible can safely fix them. We have built an astonishingly clever way to spot problems. Making sure the cure does not create another problem is a rather less glamorous achievement. [4]

AI may help catch flaws before criminals exploit them. Excellent. But discovering a weakness is not the same as repairing a live service used by millions. Imagine a doctor whose treatment cures the original complaint but leaves the patient worse off. A technology company might call it a “temporary service disruption”. The patient would probably prefer plainer English.

There is no evidence that AI caused the November outages. The more interesting question is what comes next: are businesses adopting powerful new tools faster than they are learning to manage the consequences? Progress is marvellous. Keeping the lights on remains rather important too. [1,4]

Different logos, the same plug

Choose one bank, a mobile network and a handful of online shops. You might think you have chosen independent businesses. Behind the scenes, they may share a cloud provider, a security service or a communications route. And “the cloud” is not made of vapour: it occupies buildings, burns electricity and depends on cables and people. Different logos do not always mean different risks. European banking supervisors have warned about precisely this sort of dependence. [5]

Two clocks, one customer

Engineers have one clock: it stops when the fault is fixed. Customers have another: it stops when the money arrives, the telephone works or the journey resumes. The two can be days apart.

PYRÉNÉES CAPITAL

Suite 9091, Building 15, Road 3801,
Adliya 338, Kingdom of Bahrain

+973 38873800
@ basil@pyreneescapital.com
www.pyreneescapital.com
CR No. 139655-1

On Friday 13 November, America stopped departures nationwide. Roughly five hours later, the FAA had stabilised its network and flights were moving again. That was the engineers' clock. American Airlines still had aircraft and crews in the wrong places, and passengers facing cancellations and missed connections. Recovery continued through the weekend, with a largely normal schedule expected on Monday. An afternoon's technical failure had become a weekend's logistical headache. The computers were back; the passengers were still waiting. [1]

Consider a bank transfer. Chase reported a software problem in November that delayed payments, including some involving other banks. That does not mean every receiving bank had failed. But try explaining that distinction to the shopkeeper waiting to pay a supplier. The shopkeeper needs the money, not a tour of the plumbing. [1]

Even after the technology recovers, the financial bill keeps arriving. Delta estimated that a separate global software disruption in 2024 had an approximately $500m net effect, allowing for lost revenue, extra costs and fuel savings. That is not November's bill. It does show that computers can recover considerably faster than the accounts. [6]

One bad day can become everybody's

Now imagine a payment problem arriving just as mobile service goes down. You cannot pay, cannot receive the security code and cannot call support. Shops cannot take orders. Suppliers wait. The backup plan, in a fine touch of modern irony, requires precisely the network that has stopped working.

This was not what happened in November. It is a sensible stress test for the next bad day. Large specialist providers often make each customer safer and more efficient. But when a shared service fails, the trouble can travel much further. An entire high street can find itself standing on one very sophisticated stool.

Governments and regulators are not starting from nothing. Britain, the EU and the United States already have rules or guidance intended to keep important financial services working. The question is whether the arrangements survive a real emergency. A handsome policy document may reassure the board; it is less helpful at the supermarket checkout. [8]

People can keep a little cash, write down essential numbers and agree how to contact family without an app. Sensible precautions. But nobody should need a private emergency IT department to buy groceries or reach a doctor. Essential-service providers have the bigger obligation. [8]

Is Washington spending enough? That is harder to answer than a budget headline suggests. A 2025 government watchdog report put federal IT spending above $100bn a year, much of it devoted to keeping existing systems running. Maintenance is not in itself waste. More tellingly, most of the eleven critical older systems examined lacked fully documented modernisation plans. Money matters. Knowing what it is meant to achieve matters more. [7]

Ballrooms, budgets and backup plans

Preparedness has a publicity problem. Nobody cuts a ribbon for a crisis that never happened. Working backups cost money, offer few photographs and are easy to neglect—until the saving becomes everyone else's emergency.

PYRÉNÉES CAPITAL

Suite 9091, Building 15, Road 3801,
Adliya 338, Kingdom of Bahrain

+973 38873800
@ basil@pyreneescapital.com
www.pyreneescapital.com
CR No. 139655-1

Washington's decorator-in-chief has other attractions: a ballroom, a triumphal arch, a reflecting pool and a golf-course makeover. The Center for American Progress puts taxpayer-funded spending and plans on presidential prestige projects above $2.3bn in its higher-cost scenario. That is a projection, not a bill already paid. One suspects the backup network is unlikely to compete with the chandelier for television coverage. [7]

And then there is Iran. The Pentagon initially considered seeking more than $200bn in additional war-related funding. Defence Secretary Pete Hegseth explained that "it takes money to kill bad guys". Apparently so. It also takes money — and competent planning — to keep the good guys' banks, communications and public services working. Different budgets, certainly. But Washington's willingness to contemplate vast sums makes the question of what actually works, and who answers when it fails, impossible to duck. [7]

Investors have their own reason to care. A family office may own banks, shops, logistics firms and property companies, only to discover that each depends on the same technology supplier. Diversification looks less impressive when the whole portfolio loses its password at once. What matters is how long a business can function when an essential service disappears.

Resilient power, communications and recovery services could be attractive businesses. But fashionable demand does not guarantee profitable contracts. Investors should look for companies that demonstrably reduce risk, rather than those selling a shiny new dashboard.

The greater danger may not be a single digital apocalypse. It may be that disruption becomes normal: another frozen payment, another dead mobile network, another service unavailable at precisely the wrong moment. The November incidents were separate, yet they revealed how much ordinary life rests on systems we barely notice — until they fail.

The person unable to pay for groceries should not need to discover which subcontractor disappointed which other subcontractor. The public should not need to understand the machinery to deserve protection from its failures. A service may be outsourced. Responsibility for it should not be.

Technology may fail. Accountability should not.

À bientôt, Basil

2016–2026 | Ten years of independent perspective.

About Pyrénées Capital

Pyrénées Capital is an independent Bahrain-based consultancy focused on cross-border investment origination, strategic introductions and relationships between businesses and investors. Founded in 2016, the firm works with family offices, institutions and international investment managers across markets.

www.pyreneescapital.com

PYRÉNÉES CAPITAL

Suite 9091, Building 15, Road 3801,
Adliya 338, Kingdom of Bahrain

+973 38873800
@ basil@pyreneescapital.com
www.pyreneescapital.com
CR No. 139655-1

For the curious reader

Eight short trails for readers who enjoy checking the receipts.

01 What happened in November
Microsoft · FAA · Chase · NSA

02 Cyber threats and the official response
US intelligence · White House

03 The President's own words
Trump remarks

04 AI and the danger of fixing things too quickly
Senator Warner

05 Shared systems and reliability
Uptime Institute · European Central Bank

06 When recovery takes longer than repair
American Airlines · Delta Air Lines

07 Ballrooms, budgets and backup plans
Prestige-project estimates · Iran funding proposal · Federal IT audit

08 Safeguards for ordinary people
UK regulator · EU rules · US banking guidance · UK preparedness

EDITORIAL NOTE

Public information reviewed to 19 November 2026. The November incidents were separate; no coordinated attack or common AI cause was established. The cascading-failure example is hypothetical and historical losses are not November cost estimates. Some incident findings remain preliminary. This is independent market commentary, not personalised investment advice or a securities recommendation.