the **Blackout** report

riello ups

what happens
when **there is no power?**

Written by **Christopher Owens**
Concept, design and layout by **Barry Jarvis**
Contributors **Leo Craig** & **Jason Yates**

Any enquiries regarding the content of this publication should be addressed to info@theblackoutreport.co.uk

Published by Riello UPS Ltd, U50, Clywedog Road North, Wrexham Industrial Estate, Wrexham, LL13 9XN, United Kingdom

Nine minutes after the first press of the snooze button, and with one eye half open you reach for your phone to finally turn off the alarm that you promised yourself you wouldn't sleep through again.

"Alexa, play some music" – silence...

"Alexa. Play. Some. Music" – still nothing...

Both eyes now open, the morning ritual of checking social media begins. But, nothing... no notifications, no emails. That's odd. Wait, no Wi-Fi and no mobile signal either. What's going on?

Flick the bedside lamp. Nothing. *"Ah, power cut"*.

45 minutes later, still no power but it's time to leave for work. The shower wasn't working and the toilet wouldn't flush, why does that need electric? No chance of a cup of tea and toast before heading out either. Not the best start to a Monday.

Roads seem busier than usual. Traffic lights aren't working. Guess the three-car pile-up at the junction up the road proves just how much people rely on those three coloured lights, doesn't it?

Big queue at the petrol station too, don't usually see that this time of the morning. Even a bit of a scuffle between a couple of people outside the shops, one of them carrying what must have been 10 loaves of bread – must be hungry!

Nearly at the office now... Why is everyone stood outside? Is that the security alarm? Looks like the power's out here too.

You park up and plug in your petrol-electric hybrid car. Something in the back of your mind questions why, but force of habit makes you continue anyway.

"Come on guys, put a smile on it, power will be back on soon. It always is..."

"You haven't heard, have you?"

"Heard what?"

"It's not just here, it's everywhere! The power's gone, the whole country, they say the grid's down, couple of the guys in the office were listening to the radio on the way in this morning and said it was just emergency broadcasts. Nobody's got a clue how long it'll last, someone said tomorrow or the day after, but they don't know for sure..."

CONTENTS

INTRODUCTION

What you're about to read isn't the opening to an upcoming Hollywood blockbuster or critically-acclaimed drama.

the Blackout report isn't about fiction.

It's about examining the facts.

It's about thinking the unthinkable.

And it's about asking the unanswerable questions.

Such as could there ever be a total failure of the UK electricity network?

We've never experienced one before, and our electricity network – approximately 350 substations, nearly 4,500 miles of overhead transmission lines, and almost 1,000 miles of underground cables – is designed to be as reliable and robust as possible.

However, many leading experts believe it's now simply a matter of "when, not if" such an earth-shattering event will take place. There are just too many risks, from the natural hazard of increasingly extreme weather to the double danger of cyber-attacks and terrorism.

Government, advisors, and security specialists believe the probable consequences of a severe disruption to the country's power supplies are so serious that they must be treated as the highest priority.

While such an incident remains unlikely, there's still a 1-in-200 chance it'll happen within the next five years, so it's certainly not outside the realms of possibility.

Are we fully-prepared for such a grave occurence? How do you even 'war game' for the prospect of a society without power? You can't simply cut millions of people off and turn them back on again at the mere flick of a switch.

Hundreds of millions of pounds are spent protecting our physical and digital infrastructure, but could something as seemingly trivial as not updating the default password on a connected smart device end up jeopardising our entire electricity supply?

What would really happen if the UK was plunged into darkness by a nationwide electricity blackout? It's not as straightforward as engineers working to fix faults or repair damage. If the grid does go down, it won't all come back online in a matter of minutes or even hours.

Rebooting the network requires the last resort: Black Start, a painstaking process that starts power generation again from scratch.

Because our network is becoming more and more complex, the latest high-level planning assumption is it could take as long as 5-7 days before power is fully restored and supplies begin to return to normal.

Depending on the damage, the disruption could go on for even longer. Several days with at best limited access to power and at worst no electricity whatsoever.

How would we cope in a world without power?

No email, no internet, no mobile phones, no GPS, no cash machines. It'd be like a time machine taking us back to a period pre-dating the technology that we've come to know and love, perhaps even take for granted.

The spooks at MI5 have a famous saying that we're only ever "four meals from anarchy", so it's safe to say that without electricity to store, cook, or re-stock food supplies, public order would quickly descend into chaos.

How would your business deal with such a state of calamity and confusion? In mission-critical environments, business continuity planning and risk management come as second nature. But this would be taking things to unprecedented levels.

With our way of life – and life itself – under threat, would tried-and-tested concepts such as redundancy and resilience stand strong or buckle under the pressure?

the Blackout report delves deep into all these questions and many, many more.

It's the most comprehensive analysis ever of the challenges facing data centre operators, IT administrators, risk management specialists, business continuity professionals, and anyone tasked with essential site security and disaster recovery.

WHAT ARE THE ODDS?

Odds	Event
1-in-10	A UK male living to the age of 100
1-in-100	A 9-year-old boy becoming a professional footballer
1-in-200	**Total shutdown of the UK electricity network in the next five years**
1-in-240	Dying in a road accident in the UK
1-in-285	Being killed by a firearm if you live in the USA
1-in-11,500	Winning an Oscar
1-in-12,000	An amateur golfer hitting a hole in one
1-in-10 million	Dying after being struck by lightning
1-in-11 million	Dying in a plane crash
1-in-14 million	Winning the UK lottery

SETTING THE SCENE

Why Our Evolving Energy Mix Leaves Us Vulnerable

In a modern, developed society such as the UK, it's taken for granted that when we flick the switch on a TV or one of our countless other devices and appliances, the electricity that powers our daily lives will automatically kick into action.

But quietly, behind the scenes, we're in the midst of an electrical revolution which aims to tackle the biggest challenge our planet faces – namely climate change and the need to rapidly reduce carbon emissions – whilst at the same time posing a few new power problems of its own.

For more than 100 years, the UK's electricity grid has relied on a relatively small, centralised network of large-scale power stations – predominantly coal-fired but complemented since the 1950s by nuclear plants. However around 23 GW of thermal power generation has gone offline since 2010, with a further 24 GW of coal and nuclear capacity set to close by 2025 (Howard & Bengherbi, 2016).

We're moving away from fossil fuel-generated electricity towards a future powered by renewable sources such as solar, wind, and tidal, supplemented by storing this green energy in large-scale battery installations.

Throughout 2018, power produced from renewables accounted for a record high 33% of all UK electricity. Combined with nuclear, these low-carbon sources contributed 53% of our total supplies as fossil fuels plummeted to a record low of 46% (Evans, 2019).

Since 2005, renewable energy generation has grown by 95 TWh, a trend that has helped avoid 40 megatons of CO2 emissions per year (Evans, 2019).

It was only 7 June 2017 when the UK recorded its first ever day where renewables produced more electricity than coal and gas (Harrabin, 2017).

But the first three months of 2019 alone saw the country clock up 650 hours – more than 27 days – of coal-free generation. For context, that's more than the whole of 2017 (George, 2019). May 2019 also saw the UK go coal-free for more than a week, then for a fortnight, the longest periods since the Industrial Revolution in 1882 (Jolley, 2019).

This shifting landscape comes with its own particular challenges, though. Whereas old-style power generation's main drawback is its harmful environmental impact, it delivers a reliable, predictable, and consistent output.

On the other hand, while renewables deliver undoubted benefits in terms of reduced emissions, in their present form they are far more unpredictable. Some days the wind will blow and the sun shine, some days they won't.

This uncertainty makes it increasingly difficult for National Grid to guarantee a consistent frequency, not to mention balance supply with demand.

Until the last few years, the grid has tended to have a 20% reserve between peak demand and supply. But during winter months in recent years, when renewables are at their least productive, this spare capacity has dropped as perilously low as just 1.2% (Moylan, 2015).

That's a dangerously small gap. Any unexpected energy demands – for example an extended period of extreme cold weather – could easily see an increase in mains disturbances such as brownouts and blackouts. In more extreme circumstances, electricity might need to be 'rationed' through planned Rota Disconnections.

The Era Of Interconnectivity

Just as the way we produce our power is changing, how we communicate is going through a huge transformation too. More Brits today own a smartphone than hold a driving licence.

The internet and connectivity dominate our day-to-day lives. We shop online rather than hitting the high street. We bank using our phones. We don't rely on maps or directions to get around, we use GPS instead. We scan barcodes rather than hand over paper tickets. Messaging apps bring friends from the four corners of the world together in an instant. Our smart TVs change channels at the sound of a voice, rather than a push of the button.

In the workplace, artificial intelligence, machine learning, robotics, and automation take on more and more tasks, from the monotonous (i.e. robotic production lines) to the potentially miraculous (i.e. highly-accurate AI-assisted medical diagnosis).

There are already nearly 300 million connected devices in the UK. But that amount is predicted to at least double to 625 million by 2035. Nearly three-quarters (69%) of businesses have at least 1,000 'Internet of Things' (IoT) devices on their networks. For 19% of firms, the figure is more than 10,000 (Ismail, 2019).

69% OF BUSINESSES HAVE AT LEAST 1,000 IOT DEVICES ON THEIR NETWORKS

As we head into the era of superfast 5G wireless connectivity, our reliance on the internet will only become even greater. Within the coming five years, the average person is set to interact with an IoT device 4,800 times a day (Doutriaux, 2018). To put it another way, that's once every 18 seconds.

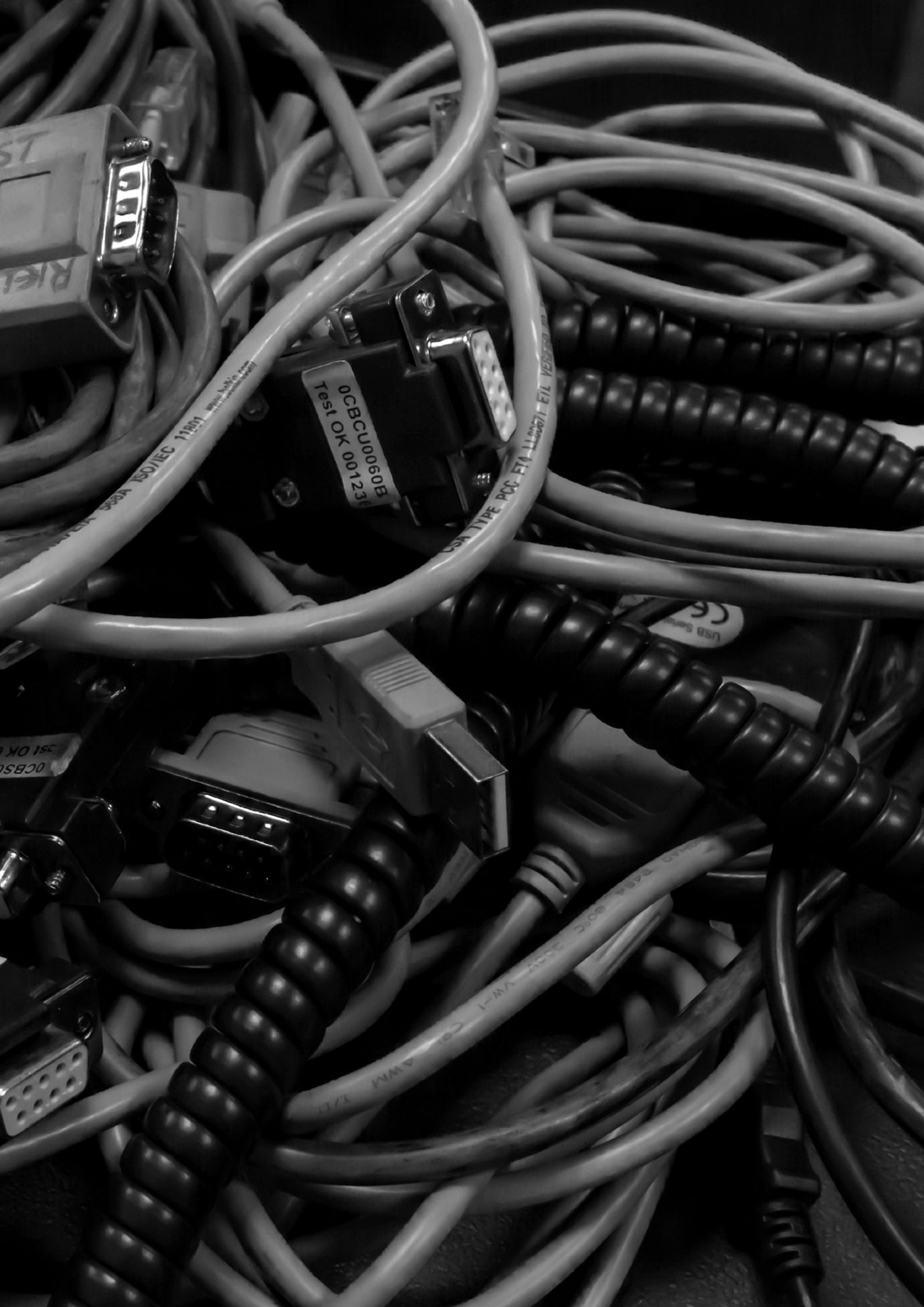
Of course, this data-driven dominance only remains practical if electricity is always there to power our Wi-Fi and telecommunications networks.

While it's arguable that society is already over-reliant on the internet, there appears to be little appetite to put that genie back into the bottle.

Instead debate centres on how an increasingly diverse, decentralised, and difficult to manage power network can keep up with society's growing technological dependency.

That task is tricky enough in its own right. But add in the growing number of serious threats to the electricity network – from natural hazards such as extreme weather through to the mounting menace of cyberwarfare – and there are fundamental questions about whether we can keep the lights on...

If we can't, is our society in any way prepared for the cataclysmic consequences of a sustained loss of power?


0CBCU0060B
Test OK 001236

POWER SUPPLY PRESSURES

By their very nature, our electricity networks are designed to be as robust and resilient as possible. According to National Grid reports, on average, UK electricity supply is available for at least 99.98% of the time (BBC, 2003).

A nationwide blackout has never happened before. But there's no room for complacency. The potential risks to our power supply have never been greater.

There are hard-to-predict natural hazards such as extreme weather or geomagnetic disturbances. There's the possibility of human error or systems failures that trigger a terrible accident. And in an increasingly volatile and divided world, we're confronted with countless man-made threats ranging from terrorist attacks on infrastructure to sophisticated cybercriminals striving to hack into and disrupt our supplies.

The 5 Biggest Threats To Our Electricity Supply

Extreme Weather & Climate Change

Climate change isn't just a threat to future generations, it's a challenge we're already facing. Scientists are seeing significant shifts both here in the UK and worldwide. Globally, average temperatures increased steadily throughout the 20th century and have continued to do so into the 21st. In fact, 2016 was the hottest year ever, more than 1ºC warmer than the pre-industrial average (National Climatic Data Center, 2017).

Here in the UK, the 10 hottest years on record have all occurred since 1990 (Daily Telegraph, 2018). February 2019 was the warmest ever and also the first time the country experienced temperatures above 20ºC on a winter's day (Butterworth, 2019).

In contrast, just 12 months previously the nation was gripped by the 'Beast from the East', a big freeze that included the coldest spring day since Met Office records began in 1910.

The underlying trends point to warmer winters and hotter summers, while sea levels around the UK's coast are rising by approximately 3mm a year as the warmer water expands and the ice caps melt (HM Government, 2017). In the years and decades to come, it's highly likely we'll experience more weather at either extreme of the spectrum – scorching temperatures, icy cold snaps, heavy rainfall, ferocious winds, and more.

All these scenarios raise the risk of serious disruption to the electricity grid, whether on a small, localised scale or at a wider regional or national level.

Howling winds or build-ups of snow bring down trees that knock out power transmission lines. Floods damage vital electrical infrastructure like substations and hinder the efforts of engineers to fix faults. Extreme temperature fluctuations lead to spikes in demand as the public relies on either air conditioning to keep cool or heaters to warm up.

By the 2080s, the Committee on Climate Change predicts the number of faults on the electricity transmission and distribution network caused by lightning alone could rise by 36% (Committee on Climate Change, 2017).

The heavy rainfall and flooding the UK saw during the winter of 2015/16, centred around Storm Desmond, offers us the best insight into the devastating disruption that severe weather can cause. But it's just one of several such examples we can refer to:

- The 'Great Storm' of October 1987 brought 15 million trees across the south-east of England crashing down, causing dozens of deaths (Gupta, 2017).
- The Burns' Day Storm in January 1990 saw gusts of 107 mph which killed 47 people across the British Isles (Met Office, 2016). While the St Jude Storm in autumn 2013 left more than 850,000 homes without power (Culf, 2013).
- In the three months between November 2015 and January 2016 alone, seven named storms caused wind damage and flooding across the UK and Ireland (Abigail, Barney, Clodagh, Desmond, Eva, Frank, and Gertrude).
- The winter of 2009-10 resulted in widespread snow building up to 20-30cm in many parts, while night-time temperatures regularly fell to -5ºC or -10ºC, even plummeting to -15ºC in the Scottish Highlands.
- Summer 2018 was the joint-hottest on record for the UK and the warmest ever for England (Met Office, 2018). A similar heatwave in August 2003 lasted for 10 days and was said to have caused 2,000 deaths. It included the country's hottest ever day, when the mercury hit a sizzling 38.5ºC in Faversham, Kent (Price, 2018).

Space Weather

Space weather is the collective term to describe a series of phenomena originating from the Sun, including asteroids, meteors, and magnetic fields.

There are three main types: **solar flares** which can reach Earth in a matter of minutes and can cause radio blackouts; slower travelling **solar energetic particles** that can produce radiation storms; and **coronal mass ejections** (CME) which are explosive eruptions of the sun that build up over four days and can lead to huge geomagnetic storms.

Our awareness of space weather dates back hundreds of years, but modern society's growing interest in the phenomenon over the last few decades coincides with our increasing dependence on signals from GPS (Global Positioning System) satellites.

Low-level space weather events happen on a regular basis, but barring a few specific industries, for example aviation, they have little impact on our day-to-day lives – apart from offering us the rare chance of catching a glimpse of the spectacular Aurora Borealis ('the Northern Lights').

However, while severe space weather events are rare, the potential impact is devastating:

- Power grid outages
- Disruption and damage to GPS and other satellite systems
- High-frequency radio communication outages
- Increased radiation at high altitude

Even a relatively weak solar flare could knock a satellite out of action. Magnetic storms can induce geoelectric fields into the Earth's lithosphere, which in turn leads to damaging voltage differentials finding their way into electricity grids through ground connections.

Historically, the largest space weather event on record seen on Earth took place in 1859.

Named after astronomer Richard Carrington, a huge magnetic storm heavily disrupted global telegraph systems and electrical equipment, with the resulting solar flare reportedly seen as far south as Mexico, Sub-Saharan Africa, and the Caribbean (Lovett, 2001).

Research suggests there's a 1% annual probability of a reoccurrence of the Carrington Event (Cabinet Office, 2015). Any repeat of such a 'Perfect Storm' today would deliver devastating disruption to many of the electrical systems and communications networks society depends on.

1989: A CORONAL MASS EJECTION CAUSED A GEOMAGNETIC STORM THAT LED TO A 9-HOUR BLACKOUT IN QUEBEC

2003: MANY SATELLITES WERE DAMAGED BY THE 'HALLOWEEN STORMS' - A SERIES OF POWERFUL SOLAR EVENTS

2012: A MASSIVE CME NARROWLY MISSED EARTH

A Carrington-scale CME was discovered by the Stereo-A satellite in July 2012 (Dr. Phillips, 2014). The path it took from the sun narrowly missed the Earth by approximately nine days.

In March 1989, a smaller magnetic storm caused the complete collapse of the Hydro-Québec electricity network in Canada, leaving nine million residents throughout the province without power for up to nine hours (Dr. Odenwald, 2009). A similar incident around Halloween in 2003 caused the UK aviation sector to lose some GPS functionality for a day (Civil Aviation Authority, 2016).

Historical records from other such space weather events in 1921 and 1960 describe extensive radio disruption and problems with railway switching and signalling systems.

Systems Failure & Large-Scale Accidents

Systems failure covers a broad category of risks from utilities malfunctions (gas, electricity, fuel, water, sewerage) through to the banking or telecoms networks crashing.

In many cases, the impact of such incidents would be restricted to a specific location or service and be dealt with locally. That's not to say there won't be knock-on effects that cause disruption to sizeable numbers of people, however.

Any widespread loss of electricity could obviously result in major disruption to most other critical systems too.

In June 2012, a faulty software update led to a massive failure at the Royal Bank of Scotland (Slater & Jain, 2013). Nearly seven million customers were unable to access phone and online banking, make cash withdrawals, or process debit card payments – proof how our society almost instantaneously grinds to a halt without simple services we've come to take for granted.

While a component fault at a wastewater treatment plant in Edinburgh left thousands of homes without access to clean water and temporarily pumped untreated sewage into the Firth of Forth at the rate of 1,000 litres a second (The Scotsman, 2007).

Similar to systems failures, industrial accidents are another broad risk category, including:

- Fires or explosions (i.e. residential and commercial buildings, power plants, refineries)
- Chemicals and biological contamination (i.e. food contamination or oil spills)
- Radiation contamination (i.e. from accidents in nuclear power stations)
- Dam breaches (i.e. flooding caused by emptying of reservoirs)

Again, the impacts of such events are most often felt – and dealt with – at a local level, although there can be wider consequences for essential services and environmental contamination, depending on the severity of the accident.

Malicious Attacks

The acute threat of terrorism is nothing new to the UK. But compared to previous incarnations, the present danger is evolving in both its origins (domestic and international) and methodology (the 'weapons' at a terrorist's disposal).

There are countless extremist groups plotting attacks on the UK and the wider western world. Home-grown terrorists radicalised by fanatical ideologies represent a growing danger from within too, whether officially trained and endorsed by terrorist organisations or acting independently but taking inspiration from their activities.

Compared to many other European nations, far-right and nationalist extremism in the UK is relatively rare, although it has seen something of an upsurge in recent years too.

In terms of risks to the nation's power supply, malicious attacks fall under two categories: Firstly, there are conventional attacks on physical infrastructure – the buildings, equipment, and distribution networks society depends on.

Then there's the growing threat of modern cyber warfare, where state or non-state actors use vulnerabilities in our increasingly tech-based systems to try and cause mass disruption, whether it's simply for financial gain or some other nefarious motive.

Infrastructure attacks

Deliberate attacks on critical infrastructure are likely to be caused by using explosives or other physical weapons, although, far more sophisticated cyber means are also part of the modern terrorist's armoury too.

Any such strike on essential networks, buildings, and infrastructure such as substations or transmission lines could lead to the crippling loss of essential services such as electricity and telecommunications.

The 1990s saw several attempts to blow-up electricity substations. The IRA also targeted Bishopsgate in the City of London in 1993 (Early, 2019) and London's Docklands in 1996 (BBC, 1996).

Further afield, terrorists have conducted concerted attacks against energy infrastructure, such as in Algeria and Yemen during 2007, 2008, and 2013 (Cabinet Office, 2017).

Another more recent example is the ongoing power struggle in Venezuela, which literally left much of the country in the dark back in spring 2019.

Anti-government forces were accused of taking out one of the main hydroelectric plants, which led to 18 out of 23 states being cut off. At its height, the power outage crippled capital city Caracas' metro system and caused the closure of the international airport (Phillips T. , 2019).

Cyber-attacks

Cyber-attacks are now an almost constant threat across all sectors of society. Analysis by Kaspersky Lab claimed there were more than 30 million cyber-attacks conducted in the UK in the last three months of 2018 alone (Hopping, 2019), while an inquiry by the House of Commons Public Accounts Committee revealed the country is more vulnerable to cyber-attacks than ever before (Evening Standard, 2019).

The economic cost of cybercrime in the UK adds up to tens of billions of pounds a year, but the impact is bigger than purely financial losses. The global WannaCry ransomware attack of 2017 infiltrated 200,000 computers in 150 countries, but it also struck notoriously vulnerable IT systems across 47 NHS Trusts, bringing chaos to GP practices and other parts of the health service.

> ***"...it is a matter of when, not if, the UK faces a serious cyber-attack***

A combination of high-grade malware and system vulnerabilities mean that cyber-attacks on critical infrastructure are no longer just the realm of a small band of elite, well-backed hackers. Today, anyone armed with just a laptop and a modicum of knowledge has the capability to launch a potentially devastating attack.

When it comes to the energy sector, there are legitimate fears over how prepared we are to thwart these growing threats. The National Cyber Security Centre has raised concerns on numerous occassions, with its CEO Ciaran Martin admitting "...it is a matter of when, not if, the UK faces a serious cyber-attack" (MacAskill, 2018).

While Steve Holliday, the former Chief Executive Officer of National Grid, told the Guardian newspaper: "Nowhere else is as worried as the UK about cyber threats. We are just off the scale on our energy system concerns on cyber" (Vaughan, 2017).

In fact, a leaked memo from intelligence agency GCHQ revealed that state-sponsored hackers – believed to be the Russian-based Dragonfly group – managed to compromise the UK's electricity system on 8 June 2017, the day of the General Election (Boren, 2016).

While the breach caused no major disruption to our power supplies at the time, it served as a warning shot across the bows.

Generally speaking, the UK's power supply has been concentrated in a relatively small number of large-scale power plants. These old-style power stations have strong physical security, use strict industry protocols, and don't tend to be connected to many outside networks, making them difficult for even experienced hackers to compromise.

This inevitably means most attempts to penetrate the grid's defences take place further down the supply chain – the various generation, transmission, and distribution systems where defences might, in theory, be easier to breach.

Our ongoing shift towards renewables-led, decentralised smart grids, combined with an increasingly internet-driven way of life, unquestionably offers potential hackers more opportunities to try and expose any vulnerabilities.

Many of the 'smart' devices used in energy technology are said to be poorly secured. Concerns have already been raised about the smart meters that energy companies are obligated to install in every home by the end of 2020. Similar cybersecurity weaknesses have been identified in everything from smart kettles to connected TVs, fridges, virtual assistants and washing machines.

Our energy system is increasingly dependent on real-time data and predictive modelling to help balance supply with demand and ensure a consistent grid frequency. As more and more of these theoretically insecure devices are connected to the network, there are inevitably more and more openings for cybercriminals to manipulate the data.

How many people realise something as simple as not updating the default password on their devices offers an easy way in for villains wanting to influence the energy grid?

Hacking into a single smart TV or kettle and switching it on might not have much of an impact. But what if it's suddenly thousands – or even millions – of devices powering up at the same time? These appliances could be turned on in the middle of the night when the network isn't expecting such a surge in demand. Or compromised devices could feed back false information to the grid, exaggerating or understating the demand for power.

Whichever way you look at it, there's the threat of spikes in local and regional power consumption that could damage grid infrastructure.

We only need to look eastwards for the most notorious case of a cyber-attack on a country's energy network.

Just before Christmas in 2015, at the height of Russia-Ukraine tensions, malware called 'BlackEnergy' shut off 30 electrical substations in Ukraine, leaving nearly 250,000 people without power for up to six hours (Greenberg, 2017).

Another major breach saw a Middle Eastern oil and gas company's safety instrumentation system infected with 'Trisis' malware, which enabled the hackers to potentially force a plant shutdown (Ranger, 2019).

Not that the western world is immune from such jeopardy. In spring 2019, the Department of Energy in the United States revealed a cyber event had affected power grids in both California and Wyoming (Sobczak, 2019).

This incident didn't cause a blackout or significantly disrupt power generation, but it was said to have seriously compromised control devices associated with the network.

32%: PERCENTAGE OF BUSINESSES AFFECTED BY A CYBER-ATTACK IN LAST 12 MONTHS

123456: STILL THE MOST COMMON PASSWORD, WHICH HAS BEEN BREACHED **23 MILLION** TIMES

£1.9 BILLION: THE AMOUNT UK GOVERNMENT IS INVESTING TO DEFEND AGAINST CYBER-ATTACKS THROUGH ITS NATIONAL CYBER SECURITY STRATEGY

150+: THE NUMBER OF COUNTRIES AFFECTED BY THE 2015 WANNACRY RANSOMWARE ATTACK

THE PROBABILITY OF POWER FAILURE

Are We Prepared For The Worst?

Although **the Blackout report** focuses on the importance of – and threats to – our electricity supply, there are a whole host of other hazards that could cause a widespread emergency in the UK.

Many of these risks might initially sound as if they come straight out of the latest Hollywood blockbuster movie or the crazed mind of a conspiracy theorist, but no matter how outlandish they appear, the Government and other agencies must plan for virtually every eventuality.

Some events have the potential to cause such widespread damage, either to life itself or our way of life, that they require a coordinated national response.

This type of incident is categorised as a 'civil emergency' and is covered by the Civil Contingencies Act 2004. This law outlines the responsibilities at both national and local level to assess, plan for, and respond to the most serious threats the country faces.

"When, Not If" – Rating The Risks

Every two years, the Government publishes a National Risk Register, its official evaluation of the most significant potential risks to the United Kingdom in the coming five years. It is based on the findings of a classified document called the National Risk Assessment (Cabinet Office, 2017).

The National Risk Register divides threats into four main categories (*natural hazards, major accidents, societal risks, and malicious attacks*) with each risk rated by its likelihood of happening and its potential impact, along with details of the preventive measures currently in place to mitigate against them.

Of course, not all risks are at the national scale. In England and Wales, Local Resilience Forums (LRFs) plan and prepare for other major threats based on local conditions, infrastructure, and geography. Regional Resilience Partnerships and Emergency Preparedness Groups carry out a similar role in Scotland and Northern Ireland respectively.

LRFs broadly follow police force boundaries and are multi-agency partnerships made up of local authorities, the NHS, the Environment Agency, and the emergency services (known as Category 1 Responders), supported by other organisations such as the Highways Agency, utilities, energy companies, and transport providers (known as Category 2 Responders).

These LRFs develop their own Community Risk Registers and Emergency Recovery Plans to prevent and mitigate the impact of any incident on their local communities.

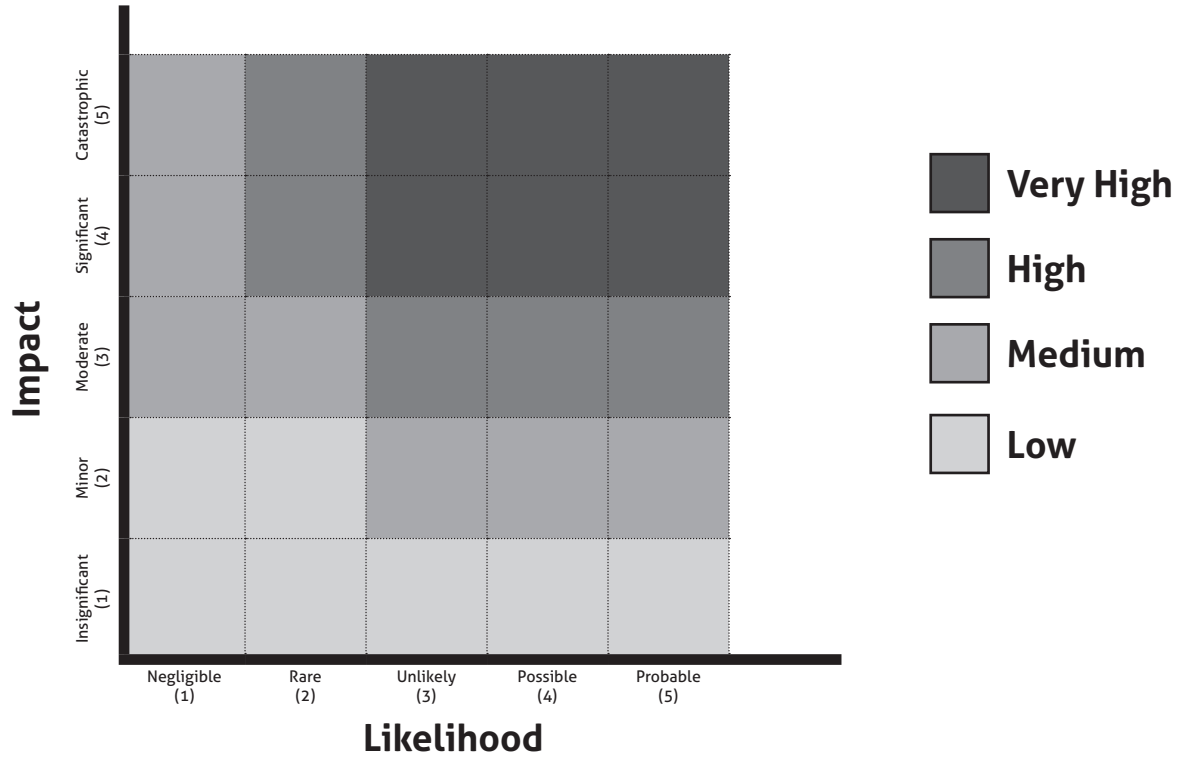
Both the National Risk Register and the various localised versions cover dozens of dangers that could cause a civil emergency. They include everything from floods, industrial accidents, and public disorder, through to terrorist attacks, infectious diseases, earthquakes, and collapsed buildings.

The likelihood and impact of all risks are each scored on a 1-5 scale. Note that the two scales are broad, to reflect the inherent uncertainty, while they are not directly comparable either.

RISK RATING

Score	Impact	Likelihood	% Likelihood (next 5 years)	Likelihood (next 5 years)
1	Limited	Low (Negligible)	0.005%	1 in 20,000 chance
2	Minor	Medium-low (Rare)	0.05%	1 in 2,000 chance
3	Moderate	Medium (Unlikely)	0.5%	1 in 200 chance
4	Significant	Medium-High (Possible)	5%	1 in 20 chance
5	Catastrophic	High (Probable)	50%	1 in 2 chance

'Impact' is calculated by taking into account the possible consequences to health (i.e. the number of fatalities, injuries, or people affected), society (i.e. disruption to services, food, the supply of money), the economy (i.e. direct and indirect costs), and the environment (i.e. long-term effect of contamination or pollution).



The various risk ratings are defined as follows:

Very high: critical risks requiring immediate attention. They may have a high or low likelihood of occurrence, but their potential consequences are so serious that they must be treated as the highest priority. Specific strategies must be in place that not only reduce or eliminate the risk, but formulate multi-agency plans to mitigate the risks if such an incident was ever to occur.

High: classed as significant. They may have a high or low likelihood of occurrence, but their potential consequences are sufficiently serious to warrant appropriate consideration.

Medium: less significant but may cause upset and inconvenience in the short-term.

Low: both unlikely to occur and not significant in their impact. They should be managed using normal or generic planning arrangements.

RATING THE RISK

These are the main risks which could directly affect electrical power supplies (Mayor of London & London Assembly, 2018)

ID	Risk Overview	Likelihood	Impact	Risk Rating
H41	Total shutdown of the UK electricity network	3	5	Very High
H45	Regional shutdown of the electricity network caused by severe weather or technical failure	3	4	Very High
H38	Rota Disconnections - emergency power cuts to balance capacity with demand	2	4	High
H56	Severe space weather equivalent to the Carrington Event of 1859, leading to widespread disruption to the electricity network	4	4	Very High
H17	Severe weather - storms and gales	3	3	High
H18	Severe weather - low temperatures and heavy snow	3	3	High
H48	Severe weather - heatwave	4	3	High
H19	Flooding - coastal/tidal	2	5	Very High
H21	Flooding - fluvial (river floods following sustained peroid of heavy rainfall)	3	4	Very High
H22	Flooding - surface water	3	3	High
X2	Physical attack on infrastructure	3	3	High
X6	Cyber-attack - infrastructure	2	3	Medium
X7	Cyber-attack - data confidentiality	5	1	Low

Preparing For Failure?

Of course, no matter how robust or even well-tested a plan is, there's no guarantee it'll ever be 100% fool-proof. That's undoubtedly the case when we're talking about something as far-reaching and fundamental as the country's electricity supply.

It's virtually impossible to 'war game' what will happen if, heaven forbid, there's a complete failure of the electricity network.

But several official documents leaked over recent years suggest we aren't as well prepared as we'd hope... or perhaps even expect.

Reports in the Daily Telegraph back in 2014 claimed that the Government's preparations for severe power cuts were based on "flawed or untested assumptions" that needed urgent revision (Gosden, 2014).

Officials across key departments undertook a test drill codenamed 'Exercise Hopkinson' to examine the outcome if a severe storm took place that knocked out power to two million homes accross the south west of England for up to a fortnight.

Even though civil servants intensely prepared for a full 12 months in the run-up to the test, the review found that any response to such a crisis would be too slow, as it would only arrive "after the local emergency resources and critical utility contingency measures had already been consumed".

One of the key failings identified in the analysis warned that fuel supplies – crucial to run backup generators and emergency response vehicles – would not be easily available for the simple fact that most petrol stations and fuel reserve bunkers rely on electric-powered pumps, which would be rendered useless without any mains supply.

> ***"It [Exercise Hopkinson] was designed to ensure emergency power plans were 'fit for purpose'. Instead it 'exposed the fact that, where contingency plans against power disruption exist, some of those plans are based on assumption rather than established fact'***

On a similar theme, leaked documents seen by the magazine Private Eye late in 2015 outlined contingency plans for a five-day UK-wide emergency power cut being drawn up by the Cabinet Office and Treasury in response to growing concerns that electricity demand would soon outstrip demand in winter months when renewable sources are at their most unreliable (Wellman, 2015).

WHAT DOES POWER FAILURE LOOK LIKE?

7 Days Of Downtime?

To date, there's never been a complete UK-wide failure of the electricity network. By design, our power grid is robust and resilient, with plenty of built-in redundancy. Critical infrastructure supplying tens of thousands of customers in our towns and cities will often be at least duplicated to ensure continuity of supply in case of serious failure or deliberate attempts to damage the network.

Over recent years, National Grid has invested £350 million improving physical security resilience and flood protection at key electricity transmission sites, with plans for a further £90 million in the coming five years. Around £30 million has been spent detecting, protecting, responding, and recovering from cyber-attacks (National Grid, 2019).

It's this deep-rooted diligence that means electricity is available to people in the UK for 99.98% of the time. But that's not to say there haven't been any recent interruptions that have affected significant parts of the country.

During the Christmas of 2013, two brutal winter storms caused such widespread damage to overhead distribution lines that 900,000 people lost power. Although the vast majority were back online inside 24 hours, 16,000 buildings were left without electricity for more than 48 hours (Cabinet Office, 2017).

Severe flooding has caused similar local and regional disruption too, notably in December 2015 when more than 60,000 properties in and around Lancaster were deprived of power for more than a day.

The incident, one of the most serious examples of a prolonged power cut on record, wasn't fully resolved for almost a week. It probably gives us the best real-life illustration of the consequences any protracted period without electricity would have. Some of the outcomes, covered later in this report, raise serious questions.

We've already seen that sustained disruption to the power network is a threat classified right at the top of the UK risk rating ('Very High'). While a total or even regional shutdown remains unlikely, at just a 1-in-200 chance within the coming five years, it certainly isn't beyond the realms of possibility.

There's a 5% (1-in-20) probability we'll experience severe space weather on a similar scale to the Carrington Event, which would undoubtedly harm our supply of power. While any of the various risks relating to flooding, extreme weather, infrastructure attacks, or cyber crime will inevitably all have knock-on effects on our electricity network too.

Overcoming A Total Power Failure

Without the benefit of a crystal ball, we can't be sure of the scale or impact any potential power blackout (either regionally focused or UK-wide) may have. It's difficult to put a timescale on how long it'll take to get back to normal without knowing the exact cause and the extent of the damage. But we can certainly make an educated guess.

The worst-case scenario is listed in the National Risk Register as the rather innocuous-sounding H41.

This is a total UK-wide power failure. It would mean the shutdown of all power stations and the wholesale loss of power generating capacity, resulting in devastating nationwide blackouts that could potentially last for days.

The recovery process from such a complete collapse is called Black Start. In effect, rebooting the entire system and kick-starting power generation again from scratch, which in itself requires huge amounts of electricity.

While it's never happened before in Britain, historically, the equivalent of a Black Start-scale incident takes place in a developed country every two years. Recent examples include Italy in 2003 (Ciuccetti & Vinci, 2003), the north east of the United States and Canada in 2003 (Holguin, 2003), and South Australia in 2016 (Harmsen, 2017).

While in June 2019, a transmission system failure left virtually the whole of Argentina, Paraguay and Uruguay - and more than 50 million people - temporarily without power (BBC, 2019).

Only a limited number of UK power stations can provide Black Start capacity. Typically, these have tended to be the old-style coal-fired plants equipped with large generators that can produce enough power on-site to restart the facility without the need for any external power.

Over time, the Black Start plants slowly produce enough electricity of their own to initially restart a skeleton network, then build up to restore the remainder of the nationwide grid.

National Grid projections suggest 60% of national electricity demand will be restored within 24 hours of a Black Start incident (National Grid, 2018). But the current risk planning assumption for a H41 event is that it could take 5-7 days for power to be completely restored.

DEPENDING ON THE DAMAGE SUSTAINED BY ELECTRICAL INFRASTRUCTURE, IN CERTAIN CASES IT COULD TAKE 14 DAYS OR EVEN LONGER.
(London Resilience Partnership, 2018)

Circumstances aren't helped by the trend towards generation from renewables. For example, most wind farms can't currently Black Start the grid because most depend on some sort of external power before they can start generating.

And even though some of the latest designs are now self-starting, they can't yet provide enough reactive power to energise the grid through the long offshore AC cables they connect with.

A Scottish Black Start Restoration Working Group review of procedures in September 2018 warned that the 2016 closure of Longannet coal-fired power plant in Fife would result in "severe delays" to the restoration of power north of the border, as it left the gas-fired facility at Peterhead as the only remaining high-power and high-inertia – crucial to stabilise frequency – power station in Scotland (Watson, 2019).

In recognition of this growing problem, National Grid is aiming to get a new procurement process for Black Start capabilities, which will incorporate renewables and even battery storage, up and running by the mid-2020s (Stoker, 2018).

The plans include allowing numerous smaller providers to join forces to meet all the eligibility requirements and encouraging network upgrades that allow for more embedded generation at low voltage levels.

Trials and pilot projects aiming to develop Black Start capabilities from distributed energy resources (DER) – another commonly-used term for renewables – are scheduled for completion by 2022 (National Grid, 2019). During 2017-18, the transmission network operator spent nearly £58 million on contracts with 18 Black Start generators.

A Localised Loss Of Power

Whilst the ramifications of a UK-wide total loss of power requiring a Black Start are clear, a more concentrated regional disruption could prove similarly catastrophic at a local level. A regional shutdown (H45 on the National Risk Register) is most likely the result of severe weather, technical failure, or operational error causing major damage to the power transmission and distribution network in a particular part of the country.

Depending on the location and severity, people could be without power for anything from 24-72 hours, with remote or rural areas likely to be cut off for several days in the worst-case scenario. In certain extreme circumstances, it could take weeks or even months for service levels to be fully restored.

While the UK as a whole hasn't had to resort to a complete Black Start scenario yet, the 'Great Storm' of October 1987 required a regional reboot after much of Kent and Sussex was left disconnected from the National Grid (Drax, 2016).

Kingsnorth Power Station, which was subsequently decommissioned in 2012, restored power across the area and ran it independently of the main grid until the wider network was repaired and reconnected.

Rationing Power Using Rota Disconnections

In either of the above scenarios – a total UK shutdown or severe regional disruption – there's a high probability that some form of power rationing will be required until the network is back approaching full capacity.

The Electricity Supply Emergency Code (ESEC) outlines the steps the Government will take to deal with serious disruption to the nation's energy supplies (Department for Business, Energy & Industrial Strategy, 2018). One of these measures involves restricting customers' consumption of electricity through what are known as Rota Disconnections – a euphemism for emergency power cuts.

Basically, the aim of Rota Disconnections is to provide as equal a distribution of electricity as possible. However, that's easier said than done in a time of crisis.

1972: A SEVEN-WEEK STRIKE BY THE NATIONAL UNION OF MINEWORKERS LED TO A POWER SHORTAGE THAT RESULTED IN MANY HOMES AND BUSINESSES BEING CUT OFF FOR UP TO NINE HOURS A DAY

First priority is what are collectively known as 'Protected Sites'. These are locations needing to have their electricity supply maintained due to public health and safety issues, because they fulfil a critical regional or national need, or because there is potential for catastrophic damage.

Protected Sites fall under three categories. 'V' stands for 'Vital Services', which are the top priority. Examples would include hospitals, airports, electricity generators and network operators, emergency services, ports and docks with national significance, railways, and postal, telecommunications, and broadcasting services.

These critical services are followed by facilities categorised as 'F' (major food manufacturers, processors, and storers) and 'O' (continuous process and manufacturing firms).

To qualify for Protected Sites status, organisations must also prove they aren't able to install their own standby power generation.

According to the ESEC, even though they are prioritised, Protected Sites must endeavour, where possible, to reduce their own consumption during a period of Rota Disconnection.

After maintaining supplies to Protected Sites, the remaining electricity is distributed equally – "as far as is reasonably practicable" – between all other customers. There's no hierarchy which states certain businesses are more important than others or that particular locations should be prioritised – it's a level playing field.

All other non-priority electricity users are divided into 18 groups or 'blocks' determined by their postcode. Each block is assigned a letter between A and U - the letters F, I, and O aren't used – while each day of the week is split into eight three-hour slots.

During Rota Disconnection, the power supply to specific blocks will be turned off for three hours at a time. The greater the shortfall in electricity, the larger number of customers who will be switched off.

Where possible, power is rationed in a way that enables businesses to operate as normally as possible for three successive days. So, for example, power cuts will be concentrated between either Monday and Wednesday or Thursday and Saturday, with Sundays shared between all blocks.

Of course, this all depends on the severity of the electricity shortage. At the lowest level of emergency, you could be without power for just three three-hour slots in a week. Conversely, if the disruption is more serious, you might be without electricity for several slots throughout the week.

Here in the UK, the most infamous case of Rota Disconnections was the "Three-Day Week" of early 1974 (Clark, 2013). While in 1972, a seven-week strike by the National Union of Mineworkers led to a power shortage that resulted in many homes and businesses being cut off for up to nine hours a day (Johnson, 1972).

Spring 2019 saw the South African government resort to similar controlled power cuts for several days to reduce pressure on the network caused by a loss of electricity imports from neighbouring Mozambique due to pylons damaged by Cyclone Idai (Hill, 2019).

Restarting The Grid From Scratch

The following estimate is based on a worst-case-scenario analysis from the Department for Business, Energy and Industrial Strategy (BEIS) of a total power outage taking place during winter, when there's little generation from renewable sources such as wind or solar (London Resilience Partnership, 2018).

National Grid contingency planning targets an average restoration time of 24 hours to reinstate 60% of national demand, providing it is "practical and cost-effective to do so".

TIMELINE OF A BLACK START

0 hours

Incident leading to total loss of power and need for Black Start restoration

0% of customers restored

0-2 hours

Black Start-capable power stations will start to come online

2-6 hours

Demand starts to be restored as Black Start power stations operate

Approximately 5% of customers restored

6-12 hours

Spread of Black Start power stations begin to join up and form a skeleton transmission network

Approximately 10% of customers restored

12-48 hours

Stable skeleton power network established

Rota Disconnections used, if necessary, to share power (Protected Sites will maintain their supplies during this period)

Approximately 60% of customers restored

2-7 days

Continuation of Rota Disconnection

Day 3: approximately 70% restored
Day 4: approximately 85% restored
Day 5: approximately 90% restored
Day 6: approximately 95% restored
Day 7: 100% customers restored in the UK

THE IMPACT OF A BLACKOUT

Catastrophic Consequences – A World Without Power

Modern life is now so reliant on electricity that a loss of power for any prolonged period of time would see society as we know it rapidly descend into chaos. No internet. No mobile phones. No petrol pumps. No contactless payments. No planes and trains, and no traffic lights on the roads.

Order would give way to anarchy. Towns and cities would become uninhabitable within days. Law and order would quickly break down as panic grows. Disease would start spreading because of a lack of sanitation and clean water.

> ***"Without electricity, modern life would grind to a halt and the complexity of modern society is such that if you take out one or two little pieces of the jigsaw, the whole thing collapses.***

Security service MI5 warns Britain is only ever "four meals away from anarchy" because any disturbance that stops the supply of food would lead to widespread looting and rioting (Fletcher-Brown, 2011).

Without electricity, food stored in fridges or freezers would quickly go off. Shops and supermarkets would either at best be quickly stripped of all supplies or at worst off limits due to tills and payment systems being unavailable.

For business, the upshot would be just as acute. Internet and email systems that dominate our working lives will fail, followed within an hour or two by the entire mobile network.

Things we take for granted in our office blocks or factories – lifts, heating, air conditioning, electronic access systems, security alarms and CCTV – will all stop working, making it increasingly uncomfortable or even unsafe for staff.

Even large-scale organisations with the backup generators and emergency supplies to keep operating for several hours – or potentially days – while the mains supply is down, will quickly become isolated and unable to function properly as the infrastructure and supply chains around them starts to crumble. Communications networks down, transport systems gridlocked, staff either unable or unwilling to come into work as alarm spreads.

While keeping companies up and running during a blackout pales in comparison to saving lives and preserving law and order, every second a business is offline, it is losing potential income, it is losing the ability to communicate with customers and suppliers, and it is potentially losing critical infrastructure or data.

According to Lord Arbuthnot of Edrom, a former chair of the House of Commons Defence Select Committee who now advises the Electric Infrastructure Security Council: "Without electricity, modern life would grind to a halt and the complexity of modern society is such that if you take out one or two little pieces of the jigsaw, the whole thing collapses" (Farmer, 2018).

Assessing The Impact

A UK-wide blackout would have immediate and far-reaching consequences across every single aspect of our lives.

Telecommunications

- Mobile phones only capable of making calls, with data to access the web, apps, or emails suspended
- Mobile network coverage likely to be lost completely within one or two hours
- The core telecoms network – old-style plug-in landlines – remains resilient for up to five days *(NB how many homes either still use a landline or have replaced their handsets with cordless versions that are useless without electricity? And with no power at the local exchange, even these landlines will be down)*
- Virtually all TV and radio broadcasts wiped out without GPS satellite signals
- BBC can provide limited updates on FM stations, but only battery-powered or car radios can receive them

Transport

- All rail, tram, and airport networks will stop running, leaving commuters trapped
- Diesel-powered bus fleets run while fuel supplies last; however, electric or hydrogen-powered vehicles will quickly become unavailable
- Traffic light failures turn the roads into a free-for-all
- Most petrol forecourts won't have the electric-powered pumps to work
- Fuel supplies quickly run out because of impaired distribution network

Healthcare

- A&E departments inundated with worried residents and people who'd usually be cared for at home or in the community
- Devices used to care for the frail and sick stop working (i.e. dialysis machines and stairlifts)
- Healthy patients can't be discharged as there's no transport to get them home
- Services reduced to just critical care and inpatient nursing
- All elective surgeries or appointments cancelled
- Severe disruption to supply chains including catering, blood and organ transplants, and medication
- Severe staff shortages due to ongoing transport difficulties and school closures
- Heightened risk of infectious disease due to lack of clean water and poor sanitation
- Deaths are inevitable: how will the dead bodies be moved, stored, and disposed of?

Households

- Immediate and ongoing loss of domestic heating, lighting, and cooking
- Even many gas-fired heating systems and cookers rely on electrical pumps or control systems to work properly
- Loss of mains tap water
- Toilets unable to flush because they too rely on electric pumps
- In around 30 hours, food spoils as turned-off fridge-freezers defrost
- Only people with battery-powered radios will receive critical updates about situation
- Only homes with old-style fixed connection landlines and corded plug-in telephones can communicate externally
- People resort to panic-buying and stockpiling with only enough food and water to last a couple of days

Businesses

- Electronic payment systems (tills and card readers) will go offline, meaning ATMs are likely to run out of cash fast
- While it lasts, cash will be king. But if the crisis runs into several days or even weeks, society could revert back to the times of a barter economy
- Banking and other financial services systems will crash
- Many buildings will close because of health and safety concerns
- Severe staff absence due to school closures and transport disruption
- Many business continuity plans assume there'll always be a critical mass of staff, but in situations like a widespread blackout, people will inevitably look after themselves and their families first
- Deliveries to supermarkets and shops will stop as fuel supplies run out

Police & Emergency Services

- Trapped people need rescuing from high-rise buildings or underground railways
- Disruption to the Criminal Justice System as the prisons, courts, and probation services grind to a halt
- Rising public disorder and looting as supplies run low
- High-risk offenders may 'disappear' because electronic tags stop working without GPS
- The special airwave communications network used by the emergency services is resilient to last for several days, but batteries require recharging for it work
- Automated alarms all trigger at the same time when the power cuts out, leaving fire and rescue struggling to determine legitimate emergencies
- Staffing in rural prisons will become a critical issue
- Thieves stealing metal from 'dead' circuits will hamper efforts to restore power unless the already-stretched military and police constantly patrol power lines

Environment

- Water treatment and sewage systems will stop functioning, leading to major issues with sanitation and clean drinking water
- Treatment works such as chlorination plants that require electricity can only run for six hours without power
- Collection of milk from the UK's 14,000+ dairy farms would become impossible
- Millions of litres of milk poured away over farms, resulting in an environmental emergency

Could Your Business Cope?

Any prolonged period without power would inevitably impact businesses of all sectors and sizes, from home-based freelancers and sole traders, through to multinational corporations with multimillion-pound turnovers and profits.

Mission-critical sites such as manufacturing plants or financial services institutions like banks or insurance firms arguably have more to lose than most.

WORRYINGLY THOUGH, ONLY AROUND HALF OF UK ORGANISATIONS (54%) ARE CONFIDENT THEY HAVE AN UP-TO-DATE BUSINESS CONTINUITY PLAN THAT THEY CAN FALL BACK ON IF THE WORST WAS TO HAPPEN
(Digitalisation World, 2019)

Modern, machine-led manufacturing relies less on manual workers and more on smart, data-driven processes. Without power, production runs come to a standstill, while wider supply chains and logistics cease to function properly.

Our tech-based finance sector would come crashing down, with people left without access to their accounts and countless automated payments or transactions failing to go through as planned.

Public services, from GP surgeries and care homes through to social security systems, are similarly dependent on databases of sensitive information requiring real-time access, analysis, and processing.

Like much of society today, these industries and services are underpinned by a nationwide cluster of data centres that store and process gigabytes of information 24/7, 365 days a year.

By the end of 2019 it's predicted there will be more than 900,000m² of server room space across the UK, the equivalent of 140 full-size football pitches (Savvas, 2018).

And while London and the M25 corridor remains the country's data centre focal point, other significant hubs are rapidly popping up in Cardiff, Newcastle, Manchester, Leeds, and Reading, to name just a few.

Whether a traditional on-site enterprise data centre or sprawling cloud-based or colocation data farm, all these mission-critical server rooms share the overarching goal of minimising downtime.

Data centres are designed in such a way to mitigate potential problems ranging from basic component failure or human error, through to widespread power loss. Most offer the resilience of redundant infrastructure, meaning that if a certain element fails there's a backup ready and able to pick up the slack.

And they employ standby power solutions such as uninterruptible power supplies (UPS) and backup generators that can deal with almost any disruption to the electrical supply, from slight sags and surges to a total power failure.

In a standard data centre set-up, the UPS system operates on its batteries whenever there's an issue with the mains, providing enough emergency backup power for servers and essential equipment to run until the standby generators – usually diesel or gas-powered – come online and take over. This can take as little as a couple of minutes, or in certain scenarios the UPS batteries could stretch to hours as a last resort.

The most well-known method for measuring data centre resilience today is known as the Tier Classification System, which was established by the Uptime Institute, a globally recognised advisory organisation. (Uptime Institute, n.d.)

This rating categorises facilities on a sliding scale of 1-4 from the most basic infrastructure to the most complex, and in theory, most resilient.

In practice, there are many more Tier III data centres than Tier IV. The sheer cost of the latter, which basically duplicates all computing and non-IT infrastructure, is prohibitive for many operators.

For both of these top two tiers, it's best practice to connect to the grid by at least two separate transformers to minimise the disruption caused if one element should fail.

Some sites will even have their power routed from two different substations or separate parts of the network to spread the risk even more. However, constructing such a diverse power infrastructure obviously comes at a considerable cost and is only a realistic choice for a select number of critical – and well-resourced – organisations.

COULD OTHER SECTORS LEARN LESSONS FROM HOW DATA CENTRES TRY TO MITIGATE THEIR POWER PROBLEMS?

UPTIME INSTITUTE TIER CLASSIFICATION

Tier Classification	Availability	Avg Annual Downtime	Overview
Tier I (Basic Capacity)	99.671%	28.8 hours	A single path for power and cooling, with few, if any redundant components. Includes a UPS and generator to protect IT from power outages.
Tier II (Redundanct Capacity Components)	99.741%	22 hours	A single path for power and cooling, plus limited redundant components including UPS modules, generators, and pumps. Provides an increased safety margin against infrastructure equipment failures plus selected maintenance opportunities.
Tier II (Concurent Maintainable - minimum N+1)	99.982%	1.6 hours	Multiple paths for power and cooling, plus enough redundant components to enable equipment to be maintained and even replaced without requiring a system shutdown. Designed to protect against power outage for at least 72 hours.
Tier IV (Fault Tolerance - minimum 2N)	99.995%	26.3 mins	Redundancy for every component across the entire computing and non-computing infrastructure. Designed to protect against power outage for at least 96 hours.

While they may not have their exact equivalent of the Tier Classification System, many industries already go to great lengths to eliminate all potential single points of failure that could bring their system crashing down.

For example, best practice guidelines for healthcare facilities focuses on the "3 Rs" (Department of Health, 2014):

ROBUSTNESS: A SYSTEM OR SITE SHOULD BE ABLE TO ABSORB THE EFFECTS OF AN EVENT AND CONTINUE TO OPERATE AT THE REQUIRED LEVEL

REDUNDANCY: IF ROBUSTNESS CANNOT BE GUARANTEED, IT IS ESSENTIAL TO PROVIDE MORE THAN ONE KEY FACILITY OR SUBSYSTEM

RECONFIGURABILITY: THE MOST DEVASTATING RISKS ARE OFTEN UNANTICIPATED. FOR TRUE RESILIENCE, A SYSTEM OR FACILITY SHOULD BE ABLE TO COPE WITH THE AFTEREFFECTS OF AN UNEXPECTED EVENT.

In practice, with the highest level grade A risks such as operating theatres, A&E departments, and critical care areas, if a disconnection to the mains supply represents a threat to life, an alternative power source must be available within half a second (or instantaneously if any break would stop an item of equipment from working).

Similar principles are adopted throughout many other mission-critical environments, from factories and refineries to water treatment works and power plants. Vital infrastructure is at least duplicated to lessen the likelihood of failure.

However, no matter how resilient a critical site is designed to be, during a sustained power outage there's only so much an operator can do to insulate themselves from disruption.

The emergency backup provided by UPS systems and generators will hold steady in the short-term, but what happens when the fuel runs out?

Even for facilities with onsite generation keeping them running, the best they can hope for is basic survival. As the days go by, these sites would be operating in isolation with a skeleton staff, little support from suppliers, and without any customers, who would have far more pressing concerns about their own situation.

Much of the maintenance is contracted out to vendors and third-parties. If any equipment encounters a problem during the blackout, who will fix it? There's no phone signal, so no means of communicating with your supplier. And even if you could, how would they be able to get to site?

It wouldn't be long until the white noise generated by the servers and cooling systems at the heart of any data centre turns into an eerie silence as operations grind to a halt.

Lessons From Lancaster

Over the first weekend of December 2015, Storm Desmond brought unprecedented flooding to parts of Cumbria and North Lancashire.

A flood at one of the main electricity substations plunged much of the city of Lancaster into a complete blackout that took nearly a week to fully resolve.

Supplies to 61,000 properties were cut and more than 100,000 people left powerless.

Only the commandeering of 75 large diesel generators, many transported from Northern Ireland or the south west of England, alleviated the problem and helped to restore power.

The incident was talked of at the time as a "1-in-100 years event" – which in hindsight could be seen as a questionable analysis based on the trend of our weather becoming more extreme and more unpredictable. But it's unquestionable that the fallout to the Lancaster blackout gives us a valuable insight into just how we'd cope with such adversity.

"Living Without Electricity", an analysis conducted by the Royal Academy of Engineering, in partnership with the Institution of Engineering and Technology and Lancaster University, catalogued the city's experience of several days without power. (Royal Academy of Engineering, 2016)

The review found a community bound together by the stereotypical 'Blitz Spirit' and camaraderie forged in times of hardship.

Shops and supermarkets handed out free food and other essentials. Volunteers at Christ Church continued running their overnight shelter for homeless people, using head torches to see what they were doing and gas cookers to provide food. The chef at a care home for the elderly built a barbeque so residents could have hot meals.

However, recovery efforts were hindered by what in isolation would be a few relatively trivial issues, but which combined added up to a population cut-off from the modern world and not really knowing what was happening.

MUCH OF THE UK'S ELECTRICAL INFRASTRUCTURE IS IN OPEN COUNTRY WHERE PROTECTION FROM A DETERMINED AND WIDESPREAD PHYSICAL ATTACK WOULD BE ALMOST IMPOSSIBLE.

Almost all mobile phone coverage was lost within an hour of the blackout starting. Even though landline services were still available, the majority of people who had replaced their traditional handsets with modern cordless models – which require electricity to work – were unable to connect.

Similarly, internet connection quickly dropped and even in parts where a signal was still available, there wasn't any electricity to power routers or Wi-Fi hubs.

Without their usual sources of news and information – TV, text message, internet, DAB radio or social media – people simply didn't know where to turn. While the old-style FM radio coverage continued to provide updates, few residents had a suitable battery-powered radio to tune in with.

Households immediately lost lighting and the power to run electrical appliances like TVs. Even though many homes had gas-fired central heating, these invariably had control systems and pumps reliant on electricity, so didn't work. Properties with all-electric cookers couldn't heat food.

Many blocks of high-rise flats used electric-powered booster pumps to transport water to the top floors. Without electricity, this accommodation had no water flowing from the taps or for flushing the toilet. The investigation also found that with no power the toilets in eco-buildings using grey water – second-hand water from showers – wouldn't flush.

TIMELINE OF A BLACKOUT

0 hours	Services with backup generators and uninterruptible power supplies will continue Closure of all other services (e.g. financial and educational)
0-2 hours	Increased demand on public services (e.g. health and social care) Closure of transport networks.
2-6 hours	After two hours the mobile phone network is likely to go down Public unable to communicate; limited radio broadcasts maintained via BBC Radio 1-4 (but how many have battery-powered radio or would think of using a car radio?)
6-12 hours	Severe staff absence begins due to transport disruption and school closures
12-48 hours	Water supply failure (some water treatment works can only last for six hours without electricity) Food in fridges and freezers will start to go off
2-7 days	After five days, the core fixed telecoms network is likely to fail Airwave network (mobile comms network used by emergency services) batteries will need to be charged Potential public disorder

Some shops and supermarkets were shut off due to restrictions on traffic across the city's river, while many others were unable to open because they didn't have the electronic means (tills or card readers) to accept payments.

Local supermarket chain Booths brought in a generator on the Sunday morning which enabled it to open as usual – the only grocery store in Lancaster that day which wasn't closed. Checkouts worked but the standalone card payment terminals didn't, so it was cash payment only.

Come 4pm, then the standard closing time on a Sunday, there were still many residents wanting to stock up on supplies. But the doors slammed shut due to inflexible Sunday trading arrangements – the report discovered nobody was aware which local or national body might have been able to relax these laws in such times of emergency.

The local hospital – Lancaster Royal Infirmary – continued functioning thanks to standby diesel generators with 14 days' worth of fuel.

However, this meant it quickly turned into an impromptu community centre for people with nowhere else to go and no other sources of information. One group of students even turned up with a six-way extension lead full of mobile phone and laptop chargers to plug into the first socket they could find to power up their precious devices!

Without access to the health service's usual first port of call of a GP, pharmacy, or 111 out of hours advice hotline, A&E predictably became a sanctuary for patients and was quickly bombarded with requests for repeat prescriptions or assistance with all sorts of non-emergency ailments.

In our increasingly aging society, more and more people now receive medical care at home. Many of these services and treatments, from stair lifts and personal alarms for the frail, through to dialysis machines or oxygen therapy, rely on either electricity or mobile phone coverage (or both).

Nursing home providers are just as reliant on electricity too. The 70-bed Laurel Bank facility in Lancaster lost heating, hot water, and lighting. Electric-powered tilting beds and chairs stopped working, while patients usually moved by electric hoists had to be manually lifted by staff instead.

Even though the care home's kitchen had a gas cooker, it was interlocked with electric-powered extractor fans and so couldn't be used.

Lancaster is situated on the West Coast Main Line (WCML) of the rail network. As the power for trains comes from feeder stations at nearby Garstang and Kendal that were unaffected by the blackout, they were able to operate as usual. The signalling and control systems were also able to work by taking power from the 25 kV traction supply and transforming it down to the necessary 600 V.

However, all the ancillary services at Lancaster railway station – the public address system, ticket machines, platform lighting, offices, and control rooms – stopped working when the power failed. Without any means to communicate with passengers or illuminate the platforms, the station was forced to close for safety reasons at 4pm each day as dusk fell.

The city's diesel-powered bus service was resilient enough to keep going almost as usual, once the bridges over River Lune had been reopened. Even then there were several issues to contend with.

The main bus station remained closed, so alternative stopping points were required. Without streetlights, passengers had to board using the internal lights on the bus.

Offices remained unlit, but staff had torches or bus headlights were used to pinpoint key locations. And even though the bus fleet was usually refuelled by electric pumps, the depot had stored several hand pumps which were used as an alternative.

While the review acknowledged the resilience of this particular bus network, it warned many other modern fleets, particularly those powered by electric or hydrogen, would struggle if ever faced with similar circumstances.

The aftermath of such a cataclysmic event invariably raises many questions, including "can we stop this from happening again?". The response to that particular question fundamentally boils down a cold, hard choice of risk versus reward.

As the report concludes, the Lancaster blackout lasted for roughly a week (2% of the year), while the city's population makes up just 0.2% of the UK population.

WHAT PRECAUTIONS – AND COSTS – ARE JUSTIFIABLE FOR SOMETHING THAT MIGHT BE REQUIRED FOR JUST 0.004% OF THE TIME?

LOOKING TO THE FUTURE

The prospect of a prolonged absence of power poses many challenging questions.

From a personal perspective, how could we as individuals, as families, as groups of friends or colleagues cope with our lives being turned completely upside down? How long would it take for things to get back to normal?

For governments, support agencies, and wider industry, the questions are much more practical – are we doing enough to prevent such an incident from taking place? And if the worst were ever to happen, are we doing everything we possibly can to minimise the devastating impact?

Moving forward, there are several key trends that will influence both the likelihood of society experiencing a major electricity network failure and how we try to prepare for such an eventuality.

Even Greater Internet Dependence

The developed world is heading into the era of superfast 5G. With the capability to support 1,000 more devices per square metre than its 4G predecessor and the promise of download speeds 1,000 times quicker too, our enslavement to the internet and connectivity is set to intensify as concepts such as the 'Internet of Things', 'Smart Cities', 'Industry 4.0', and 'Smart Grids' take an irreversible stranglehold on our personal and professional lives.

Naturally, the better the internet becomes, the more we'll rely on it. And while there's no holding back progress, we must never forget that the internet is at the mercy of the electricity that powers it.

As we've seen, if something takes that power offline, the entire system rapidly unravels at the seams.

Yes, there are already national and local-level risk registers and strategies in place to protect people, businesses, and wider society against the biggest dangers.

But for something as all-consuming as a nationwide power loss, do we need to take these preparations one stage further?

Should businesses and organisations above a certain size be compelled – by law if necessary – to draw up worst-case scenario plans? Perhaps they could be forced to structure their operations to minimise unnecessary power usage during an emergency?

For mission-critical sites such as data centres, these plans could even extend to minimising the electricity required so they are able to prolong critical services during a sustained power outage. A benefit of this would be to alleviate any unnecessary load on the backup generators, helping conserve fuel so it lasts longer.

Surely given the choice between two admittedly desperate options, businesses would much rather run just their most critical services and operations, as opposed to than suffering a complete shutdown?

Road To Renewables Offers Risks And Rewards

In the next 10-20 years, our electricity network will be unrecognisable from the structure we've become used to over the last 100 years.

The days of a small number of power stations feeding power through cables and transformers are numbered. Up to 65% of power generation could be localised by 2050 (National Grid, 2018).

Distributed generation from wind turbines, solar panels, and other renewable sources will become the norm, rather than the exception.

Instead of a passive grid only carrying power to consumers in one direction, we'll have an active bi-directional network linking several smart grids of users deploying devices such as smart meters and Wi-Fi operated thermostats.

Rather than controlling power generation to meet demand, we'll be controlling the demand to meet the supply, with energy users potentially becoming producers too.

Does this more diverse grid promise greater resilience or simply provide far more opportunities for failure, particularly in terms of cyber-attacks?

Since 2018, organisations involved in essential services and digital infrastructure are now subject to the Network and Information Systems Regulations (NIS Regulations), legal measures aimed at enhancing the level of physical and cyber security across our information systems. Will these protocols be enough to keep cybercriminals at bay?

As well as the environmental advantage, the move towards distributed energy resources does offer another potential benefit.

As more and more homes, businesses, and organisations install their own solar panels, wind turbines, biomass, and other onsite generation, does it open the door for locally-generated off grid electricity that can support the most basic of systems during a major regional or national power incident?

This would undoubtedly be helped if more homeowners were encouraged to combine their solar panels with battery storage to enable them to fully harness their onsite generation.

Of course, domestic energy storage isn't necessarily suitable for every installation, but for properties with a large number of solar panels – or residents who aren't always there during the day to use the electricity – lithium-ion batteries such as Tesla Powerwall offer significant upside.

What Price Do We Put On Our Way Of Life?

We're used to weighing up pros and cons – do we feel safe flying in an aeroplane? Should we take out life insurance?

Likewise, every day we make countless choices about value for money – is that product or service really worth what we're paying for it?

At face value, protecting our electrical infrastructure boils down to those same fundamental decisions. Is the cost of guaranteed electricity a price worth paying?

Of course, it's not quite the same as whether you choose to buy a new car or not, or weighing up which of two competing brands to purchase from.

As we've seen, the probability of a nationwide blackout is still extremely unlikely – just a 0.5% chance in the next five years. But we also know if it did ever happen, the economic and societal costs would be enormous. That's why we need to take every necessary precaution to prevent it from occurring.

Making our electricity network more secure and reliable inevitably costs a lot of money.

How comfortable are we – as taxpayers and as consumers – to shell out for something that we hope we'll never need? We might consider our modern way of life priceless, but how much are we willing to pay for the ultimate insurance to keep it that way?

There's little political capital to be gained for telling people the harsh truth in situations as complex as this. The public at large believes the lights will always come on when they flick the switch and has little interest in the nuances – or the hard work going on behind the scenes – that ensure this happens the overwhelming majority of the time.

As well as asking how much we should pay, we also need to establish who should pay. The taxpayer alone can't carry the burden, but what would a fair contribution from industry be?

For example, internet and mobile communications providers are in an unenviable position when it comes to ensuring a reliable service in case of a power failure. How do they justify the massive investment (millions or even billions of pounds) to protect against a "once in a lifetime" event or something that might never actually happen?

Would A Publicly-Owned Power Grid Make A Difference?

Could the way our electricity network is owned and operated have much of an impact? Calls to bring National Grid back under public ownership have been made ever since the network was first privatised in 1990.

But renationalisation of energy has gained wider public and political support in recent years, perhaps as a populist backlash to rising household bills at the same time as energy companies have been posting gigantic profits and paying huge dividends to shareholders.

Rather than looking at nationalisation as fighting some sort of class warfare, should our electricity network be viewed through an entirely different prism – namely infrastructure of such strategic importance that it should operate above the influence of market forces?

National Grid claims electricity transmission only costs every household in the UK around 4.5% – approximately £25 – of its average annual electricity bill (National Grid, 2019). It will point to the hundreds of millions of pounds it has invested in improving the network over recent decades.

This includes £350 million spent improving resilience at key sites plus £100 million on upgrading flood defences and £30 million on cybersecurity, all in the period 2013/14 to 2020/21 covered by the RIIO-T1 framework. Equally vast sums will undoubtedly be allocated in RIIO-T2 from 2021 too.

But what can't be denied is that the energy network as a whole has handed out billions of pounds to shareholders over the past decade (Wild, 2017), money critics argue could have been spent on upgrading vital infrastructure instead.

Would a National Grid – and for that matter Distribution Network Operators – that put the interests of the public before profits be better placed to deliver a modern, decentralised, smart electricity network that prioritises safety, security, and continuity of supply?

Or is the continued role of markets and shareholders – many of whom are internationally-based – the only viable way to ensure investment in our infrastructure keeps pace, even if it does raise questions about democratic control and where the overall priorities lie?

Perhaps the solution lies somewhere in the middle. The private sector continuing to own and run the network, but with increased oversight from the Government – backed by additional powers for regulators like Ofgem or even new legislation if required – to ensure they make the necessary investment and have the robust contingency plans in place to both reduce the risk and mitigate the impact of any major failure.

It isn't the role of **the Blackout report** to come to any firm conclusions. That responsibility lies in the hands of politicians, regulators, and the power industry itself.

However, several key questions crop up time and time again throughout this report:

- Are we fully-prepared for the ever-changing threats we face?
- Have emergency plans been tested rigorously enough?
- Would our response be sufficient?

It's unclear whether the answers we have at present are satisfactory. In honesty, the evidence suggests otherwise.

There are no silver bullets or simple solutions to such a complex and fundamental challenge as keeping the power on.

But neither is any complacency acceptable – this report proves beyond doubt that the view "this could never happen to us" is a dangerously naïve belief.

Whether we're a data centre operator, a risk management advisor, a civil servant charged with putting together contingency plans, or simply an office worker going about our day-to-day lives, none of us are invincible.

IN A WORLD WITHOUT POWER, HOW DO WE SURVIVE?

REFERENCES

BBC. (1996, February 10). 1996: Docklands bomb ends IRA ceasefire.
Retrieved from BBC: http://news.bbc.co.uk/onthisday/hi/dates/stories/february/10/newsid_2539000/2539265.stm

BBC. (2003, August 29). Q&A: The National Grid.
Retrieved from BBC: http://news.bbc.co.uk/1/hi/uk/3191323.stm

BBC. (2019, June 17). Argentina and Uruguay reel after massive power outage.
Retrieved from BBC: https://www.bbc.co.uk/news/world-latin-america-48652686

Boren, Z. (2016, June 11). Dragonfly: How Britain's energy sector was hacked.
Retrieved from Unearthed: https://unearthed.greenpeace.org/2018/06/11/dragonfly-uk-energy-hacker-cybersecurity/

Butterworth, B. (2019, February 25). Met Office says it's the hottest February day since records began.
Retrieved from The i: https://inews.co.uk/news/uk/uk-weather-forecast-met-office-spring-warm-temperatures-february-heatwave/

Cabinet Office. (2015). Space Weather Preparedness Strategy. London: Cabinet Office.
Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/449593/BIS-15-457-space-weather-preparedness-strategy.pdf

Cabinet Office. (2017). National Risk Register Of Civil Emergencies (2017 edition). London: Cabinet Office.
Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

Ciuccetti, E., & Vinci, A. (2003, September 28). Italy recovering from big blackout.
Retrieved from CNN: http://edition.cnn.com/2003/WORLD/europe/09/28/italy.blackout/index.html

Clark, N. (2013, November 21). The Last Big Blackout: 40 years ago the lights really did go off.
Retrieved from Daily Express: https://www.express.co.uk/news/uk/444213/The-Last-Big-Blackout-40-years-ago-the-lights-really-did-go-off

Civil Aviation Authority. (2016). Impacts of space weather on aviation. London: Civil Aviation Authority.
Retrieved from https://publicapps.caa.co.uk/docs/33/CAP%201428%20JUL16.pdf

Committee on Climate Change. (2017). UK Climate Change Risk Assessment 2017 Evidence Report (Summary for England). London: Committee on Climate Change.
Retrieved from https://www.theccc.org.uk/wp-content/uploads/2016/07/UK-CCRA-2017-England-National-Summary-1.pdf

Culf, A. (2013, October 28). UK death toll mounts as St Jude storm leaves trail of destruction.
Retrieved from Guardian: https://www.theguardian.com/uk-news/2013/oct/28/britain-storm-winds-death-flooding

Daily Telegraph. (2018, July 31). Top 10 hottest years in UK have happened since 1990.
Retrieved from Daily Telegraph.

Department for Business, Energy & Industrial Strategy. (2018). Electricity Supply Emergency Code (ESEC). London: Department for Business, Energy & Industrial Strategy.
Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/698739/2018_03_29_Electricity_Supply_Emergency_Code__ESEC__2018_Revision_V1.0-.pdf

Department of Health. (2014). Health Building Note 00-07 - Planning for a resilient healthcare estate. London: Department of Health.
Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/306367/HBN_00-07-250414.pdf

Digitalisation World. (2019, May 14). Only half of UK organisations are confident their business continuity plan is up-to-date.
Retrieved from Digitalisation World: https://digitalisationworld.com/news/56905/only-half-of-uk-organisations-are-confident-their-business-continuity-plan-is-up-to-date

Doutriaux, E. (2018, March 29). Smart storage: why you should think about backing up.
Retrieved from Computer Business Review: https://www.cbronline.com/opinion/smart-storage-think-backing

Dr. Odenwald, S. (2009, March 13). The Day The Sun Brought Darkness.
Retrieved from NASA: https://www.nasa.gov/topics/earth/features/sun_darkness.html

Dr. Phillips, T. (2014, July 23). Near Miss: The Solar Superstorm Of July 2012.
Retrieved from NASA: https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm

Drax. (2016, October 16). Black Start: the most important back up plan you've never heard of.
Retrieved from Drax: https://www.drax.com/technology/black-start-important-back-plan-youve-never-heard/

Early, C. (2019, April 23). April 24 1993: IRA's Bishopsgate bomb devastates the heart of the City of London.
Retrieved from BT: https://home.bt.com/news/on-this-day/april-24-1993-iras-bishopsgate-bomb-devastates-the-heart-of-the-city-of-london-11363977172852

Evans, S. (2019, January 3). Analysis: UK electricity generation in 2018 falls to lowest level since 1994.
Retrieved from Carbon Brief: https://www.carbonbrief.org/analysis-uk-electricity-generation-2018-falls-to-lowest-since-1994

Evening Standard. (2019, June 5). Cyber-attack threat: UK more vulnerable than ever before, Commons report warns.
Retrieved from Evening Standard: https://www.standard.co.uk/news/uk/cyber-attack-threat-uk-more-vulnerable-than-ever-before-commons-report-warns-a4159631.html

Farmer, B. (2018, March 17). Four meals from anarchy: How Britain would collapse in just days if power supply is cut.
Retrieved from Daily Telegraph: https://www.telegraph.co.uk/news/2018/03/17/britain-four-meals-away-anarchy-cyber-attack-takes-power-grid/

Fletcher-Brown, M. (2011, October 16). Riots: Remember the Four Meal Rule.
Retrieved from Huffington Post: https://www.huffingtonpost.co.uk/mark-fletcherbrown/riots-remember-the-four-m_b_927882.html

George, S. (2019, April 15). UK breaks coal-free power generation record by huge margin.
Retrieved from Euractiv: https://www.euractiv.com/section/energy/news/uk-breaks-coal-free-power-generation-record-by-huge-margin/1332967/

Gosden, E. (2014, December 28). Britain unprepared for severe blackouts, secret Government report reveals.
Retrieved from Daily Telegraph: https://www.telegraph.co.uk/news/earth/energy/11311725/Britain-unprepared-for-severe-blackouts-secret-Government-report-reveals.html

Greenberg, A. (2017, June 20). How An Entire Nation Became Russia's Test Lab For Cyberwar.
Retrieved from Wired.com: https://www.wired.com/story/russian-hackers-attack-ukraine/

Gupta, T. (2017, October 15). Great Storm 1987: The day 18 people were killed.
Retrieved from BBC: https://www.bbc.co.uk/news/uk-england-kent-41366241

Harmsen, N. (2017, March 28). AEMO releases final report into SA blackout, blames wind farm settings for state-wide power failure.
Retrieved from ABC (Australian Broadcast Corporation): https://www.abc.net.au/news/2017-03-28/wind-farm-settings-to-blame-for-sa-blackout-aemo-says/8389920

Harrabin, R. (2017, June 8). Renewables provide more than half UK electricity for first time.
Retrieved from BBC: https://www.bbc.co.uk/news/business-40198567

Hill, M. (2019, March 20). Mozambique Power Links To Restore South Africa May Take Weeks To Restore.
Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2019-03-20/mozambique-power-links-to-south-africa-may-take-weeks-to-restore

HM Government. (2017). UK Climate Change Risk Assessment 2017. London: HM Government.
Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584281/uk-climate-change-risk-assess-2017.pdf

Holguin, J. (2003, August 15). Biggest blackout in U.S. history.
Retrieved from CBS News: https://www.cbsnews.com/news/biggest-blackout-in-us-history/

Hopping, C. (2019, January 21). Kaspersky Lab: 30 million cyber-attacks hit the UK at the end of 2018.
Retrieved from IT Pro: https://www.itpro.co.uk/security/32794/kaspersky-lab-30-million-cyber-attacks-hit-the-uk-at-the-end-of-2018

Howard, R., & Bengherbi, Z. (2016). Power 2.0 - Building a smarter, greener, cheaper electricity system. London: Policy Exchange.
Retrieved from https://policyexchange.org.uk/wp-content/uploads/2016/11/POWER-2.0.pdf

Ismail, N. (2019, February 20). 2.8m UK businesses vulnerable to IoT and OT cyber-attacks.
Retrieved from Information Age: https://www.information-age.com/uk-businesses-iot-ot-cyber-attacks-123479373/

Johnson, H. (1972, February 16). Blackouts will total nine hours daily.
Retrieved from Guardian: https://www.theguardian.com/theguardian/1972/feb/16/fromthearchive

Jolley, J. (2019, May 8). Britain passes one week without coal power for first time since 1882.
Retrieved from Guardian: https://www.theguardian.com/environment/2019/may/08/britain-passes-1-week-without-coal-power-for-first-time-since-1882

London Resilience Partnership. (2018). London Power Supply Disruption Framework. London: London Resilience Partnership.
Retrieved from https://www.london.gov.uk/sites/default/files/london_power_supply_disruption_framework_v3.1_october_2018.pdf

Lovett, R. A. (2001, May 2). What If The Biggest Solar Storm On Record Happened Today?
Retrieved from National Geographic: https://www.nationalgeographic.co.uk/space/what-if-biggest-solar-storm-record-happened-today

MacAskill, E. (2018, January 23). Major cyber-attack on UK a matter of 'when, not if' - security chief.
Retrieved from Guardian: https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin

Mayor of London & London Assembly. (2018, February). London Risk Register.
Retrieved from Mayor of London & London Assembly: https://www.london.gov.uk/sites/default/files/london_risk_register_v7.pdf

Met Office. (2016, April 15). Burns' Day Storm - 25 January 1990.
Retrieved from Met Office: https://www.metoffice.gov.uk/binaries/content/assets/metofficegovuk/pdf/weather/learn-about/uk-past-events/interesting/1990/burns-day-storm---25-january-1990---met-office.pdf

Met Office. (2018, August 31). Was summer 2018 the hottest on record?
Retrieved from Met Office: https://www.metoffice.gov.uk/about-us/press-office/news/weather-and-climate/2018/end-of-summer-stats

Moylan, J. (2015, July 15). Electricity blackouts risk up, says National Grid.
Retrieved from BBC: https://www.bbc.co.uk/news/business-33527967

National Climatic Data Center. (2017). NOAA National Centers for Environmental Information, State of the Climate: Global Climate Report for Annual 2016.
Retrieved from https://www.ncdc.noaa.gov/sotc/global/201613

National Grid. (2018, April). Black Start Strategy. Warwick: National Grid.
Retrieved from National Grid: Black Start Strategy: https://www.nationalgrideso.com/sites/eso/files/documents/Black%20Start%20Strategy%20Version%202%20April%202018.pdf

National Grid. (2018). Future Energy Scenarios in five minutes. Warwick: National Grid.
Retrieved from http://fes.nationalgrid.com/media/1357/fes-2018-in-5-minutes-web-version.pdf

National Grid. (2019, March 25). Breaking Down Your Electricity Bill.
Retrieved from National Grid: https://www.nationalgridet.com/about-us/breaking-down-your-bill

National Grid. (2019, March 29). Project Distributed Restoration.
Retrieved from National Grid: https://www.nationalgrideso.com/project-black-start-from-der

National Grid. (2019). Shaping the electricity transmission system of the future. Warwick: National Grid.
Retrieved from https://www.nationalgridet.com/document/129316/download

Ofcom. (2018). Protecting Access To Emergency Organisations When There Is A Power Cut At The Customer's Premises.
Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0016/123118/guidance-emergency-access-power-cut.pdf

Phillips, T. (2019, March 8). Venezuela: huge power outage leaves much of country in the dark.
Retrieved from Guardian: https://www.theguardian.com/world/2019/mar/07/venezuela-hit-by-major-power-outage

Price, C. (2018, July 27). Faversham records highest temperature in UK this year.
Retrieved from Kent Online (Kent Messenger Newspaper): https://www.kentonline.co.uk/faversham/news/kent-records-uks-hottest-temperature-187094/

Ranger, S. (2019, June 14). This 'most dangerous' hacking group is now probing power grids.
Retrieved from ZDNet: https://www.zdnet.com/article/this-most-dangerous-hacking-group-is-now-probing-power-grids/

Royal Academy of Engineering. (2016). Living Without Electricity: One city's experience of coping with loss of power. London: Royal Academy of Engineering.
Retrieved from https://www.raeng.org.uk/publications/reports/living-without-electricity

Savvas, A. (2018, September 21). Data Centre Prices Rapidly Go Up In European Hotspots Says Trend Watcher.
Retrieved from Data Economy: https://data-economy.com/data-centre-prices-rapidly-go-up-in-european-hotspots-says-trend-watcher/

Slater, S., & Jain, A. (2013, December 3). RBS admits decades of IT neglect after systems crash.
Retrieved from Reuters: https://uk.reuters.com/article/uk-rbs-technology/rbs-admits-decades-of-it-neglect-after-systems-crash-idUKBRE9B10YB20131203

Sobczak, B. (2019, May 6). Experts assess damage after first cyberattack on U.S. grid.
Retrieved from E&E News: https://www.eenews.net/stories/1060281821/

Stoker, L. (2018, May 31). National Grid outlines plans for competitive, distributed energy-friendly Black Start procurement.
Retrieved from Current News: https://www.current-news.co.uk/news/national-grid-outlines-plans-fopr-competitive-distributed-energy-friendly-black-start-procurement

The Scotsman. (2007, April 23). Enough effluent to fill 170 swimming pools pours into Forth from sewage plant.
Retrieved from The Scotsman: https://www.scotsman.com/news-2-15012/enough-effluent-to-fill-170-swimming-pools-pours-into-forth-from-sewage-plant-1-744307

Uptime Institute. (n.d.). Tier Classification System.
Retrieved from Uptime Institute: https://uptimeinstitute.com/tiers

Vaughan, A. (2017, June 26). UK energy industry cyber-attack fears are 'off the scale'.
Retrieved from Guardian: https://www.theguardian.com/technology/2017/jun/25/uk-electricity-grid-cyber-attack-risk-energy-industry

Watson, D. (2019, March 11). Market failures could see Britain suffering five-day power cuts.
Retrieved from E&T Magazine (Engineering & Technology): https://eandt.theiet.org/content/articles/2019/03/market-failures-could-see-britain-suffering-five-day-power-cuts/

Wellman, A. (2015, November 4). Secret government plans for 5-day power cut 'would knock out landlines, phones, public transport and streetlights'.
Retrieved from Daily Mirror: https://www.mirror.co.uk/news/uk-news/government-contingency-plans-5-day-6767579

Wild, M. (2017). Energy Consumers' Missing Billions. London: Citizens Advice.
Retrieved from https://www.citizensadvice.org.uk/Global/CitizensAdvice/Energy/EnergyConsumersMissingBillions.pdf

www.riello-ups.co.uk

the
Blackout report

www.theblackoutreport.co.uk