LLOYD'S

Emerging Risk Report – 2015
Innovation Series

SOCIETY & SECURITY

Business Blackout

The insurance implications of a cyber attack on the US power grid

Centre for
Risk Studies
UNIVERSITY OF CAMBRIDGE
Judge Business School

About Lloyd's

Lloyd's is the world's only specialist insurance and reinsurance market that offers a unique concentration of expertise and talent, backed by strong financial ratings and international licences. It is often the first to insure new, unusual or complex risks, providing innovative insurance solutions for local, cross border and global risks. Its strength lies in the diversity and expertise of the brokers and managing agents working at Lloyd's, supported by capital from across the world. In 2015, more than 90 syndicates are underwriting insurance and reinsurance at Lloyd's, covering all lines of business from more than 200 countries and territories worldwide. Lloyd's is regulated by the Prudential Regulatory Authority and Financial Conduct Authority. Business Blackout is an Emerging Risk report published by Lloyd's as part of its Innovation Series.

Key contacts

Trevor Maynard
Head, Exposure Management & Reinsurance
trevor.maynard@lloyds.com

Nick Beecroft
Manager, Emerging Risks & Research
nick.beecroft@lloyds.com

For general enquiries about this report and Lloyd's work on emerging risks, please contact
emergingrisks@lloyds.com

Disclaimer

Contents

Materials accompanying this report, available online:

Appendix 1: Guide to insurance portfolio loss estimation – www.lloyds.com/PortfolioLossEstimation

Appendix 2: Technical report: scenario design and impact modelling methodologies – www.lloyds.com/ScenarioDesign

Cambridge Centre for Risk Studies
University of Cambridge Judge Business School
Trumpington Street
Cambridge, CB2 1AG
United Kingdom
enquiries.risk@jbs.cam.ac.uk
www.risk.jbs.cam.ac.uk/

May 2015

Erebos Cyber Blackout Scenario Research Project Team

Simon Ruffle, Director of Technology Research & Innovation, Project Lead
Éireann Leverett, Senior Risk Researcher
Dr Andrew Coburn, Director of Advisory Board, Centre for Risk Studies, and Senior Vice President of RMS Inc.
Jennifer Copic, Research Assistant
Dr Scott Kelly, Senior Research Associate
Tamara Evan, Contributing Editor

Cambridge Centre for Risk Studies Research Team

Professor Daniel Ralph, Academic Director
Dr Michelle Tuveson, Executive Director
Dr Olaf Bochmann, Research Associate
Dr Louise Pryor, Senior Risk Researcher
Jaclyn Zhiyi Yeo, Research Assistant

Acknowledgements
The research project team gratefully acknowledges the inputs and assistance of the following reviewers and contributors. All errors and interpretations of the advice received are however entirely those of the Cambridge research team.

Nick Beecroft, *Lloyd's*
Joe Hancock, Rick Welsh and Neville Drew, *Aegis*
Tom Hoad, *Tokio Marine Kiln*
James Nevitt and Russell Kennedy, *Brit Insurance*
Dr Mike Maran, *XL Catlin*
Russell Bean, Jahangez Chaudhery, Benjamin Kiely, David Spratt, Charity Bare, *Talbot Validus*
Dr Bob Reville and Dr RJ Briggs, *Praedicat*
Dr Gordon Woo, Peter Ulrich and Paul VanderMarck, *RMS Inc.*
James Snook, *UK Government, Cabinet Office*
Jason Larsen, *IOActive*
Tim Yardley, *University of Illinois Urbana-Champaign*
Tim Roxey and Ben Miller, *North American Electric Reliability Corporation; Electricity Sector Information Sharing and Analysis Center (ES-ISAC)*
Tom Finan, *Department of Homeland Security, United States Government*
Dr Richard Clayton and Dr Frank Stajano, *Cambridge Computer Laboratory, University of Cambridge*
Chris Sistrunk, *Mandiant*
Michael Toecker, *Context*
Robert M Lee, *Dragos Security*

We are also grateful to other contributors who preferred not to be cited.

Foreword

Surveys suggest that cyber is an under-insured risk: many more organisations believe that their existing insurance would respond in the event of cyber attack than is likely to be the case.[1] Understanding the impact of severe events is one of the key requirements for insurers to develop cyber risk cover, and this study aims to contribute to that knowledge base.

The scenario described in the report reveals three attributes of cyber risk that are particularly significant for the development of insurance solutions. These factors may individually be found in a variety of risks, but cyber risk combines them in ways that demand innovative responses by insurers.

The first of these is systemic exposure. Digital networks and shared technologies form connections that can be exploited by attackers to generate widespread impacts. The hostile actors described in this report are motivated to create broad disruption to the US economy, and cyber attack against the power grid serving New York and Washington DC provides them a means to achieve it. The analysis suggests that insurers could be required to meet claims across many different classes of cover, which emphasises the importance of insurers applying robust exposure management for cyber risk across the entire portfolio.

The second key attribute is the fact that cyber attack is an intangible peril. Studies have revealed that victims often only become aware that they have been targeted months or even years after the event, and that the location of a cyber security breach on a network is often never determined.[2] In this scenario, malware is inserted into the target systems without being detected and lies dormant for several months. In the aftermath, a full year of investigation is required to understand the true nature of the attack, and the perpetrators are never positively identified. For insurers, these factors present challenges for assessing risk exposure for any given entity and in aggregate across the portfolio.

Third is the dynamic nature of the threat. Cyber attacks are often treated as a problem of technology, but they originate with human actors who employ imagination and surprise to defeat the security in place. The evidence of major attacks during 2014 suggests that attackers were often able to exploit vulnerabilities faster than defenders could remedy them.[3] In order to achieve accurate assessment of risks, insurers need insight into the evolution of tactics and motives across the full spectrum of threats.

For insurers, responding to these challenges will demand innovative collaborations harnessing multi-disciplinary expertise. Key requirements will be to enhance the quality of data available and to continue the development of probabilistic modelling for cyber risk. Sharing of cyber attack data and pooling of claims information is a complex issue, but the systemic, intangible, dynamic nature of cyber risk means that all parties involved in managing the risk have an interest in sharing anonymised data on the frequency and severity of attacks.

This report reveals a complex set of challenges, but the combination of insurers' expertise in pricing risks together with the capabilities of the cyber security sector to assess threats and vulnerabilities, and the risk modelling expertise of the research community, has the potential to offer a new generation of cyber insurance solutions for the digital age.

Tom Bolt
Director, Performance Management
Lloyd's

[1] *HM Government & Marsh (2015)*

[2] *See for example Ponemon Institute (2015)*

[3] *Symantec (2015)*

Executive summary

"A trusted component or system is one which you can insure." (Ross J Anderson, "Liability and Computer Security: Nine Principles", ESORICS 1994, p.244)

Overview

Business Blackout, a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies, considers the insurance implications of a cyber attack on the US power grid.

While there have been large individual business losses attributed to cyber attacks, there have, at the date of writing, been no examples of catastrophe-level losses from a widespread cyber attack affecting many companies and insurers at the same time.

This report publishes, for the first time, the impacts of this sort of attack using the hypothetical scenario of an electricity blackout that plunges 15 US states including New York City and Washington DC into darkness and leaves 93 million people without power. The scenario, while improbable, is technologically possible and is assessed to be within the benchmark return period of 1:200 against which insurers must be resilient.

The scenario predicts a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail and chaos to transport networks as infrastructure collapses.

In the scenario, a piece of malware (the 'Erebos' trojan) infects electricity generation control rooms in parts of the Northeastern United States. The malware goes undetected until it is triggered on a particular day when it releases its payload which tries to take control of generators with specific vulnerabilities. In this scenario it finds 50 generators that it can control, and forces them to overload and burn out, in some cases causing additional fires and explosions. This temporarily destabilises the Northeastern United States regional grid and causes some sustained outages. While power is restored to some areas within 24 hours, other parts of the region remain without electricity for a number of weeks.

Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain. The total impact to the US economy is estimated at $243bn, rising to more than $1trn in the most extreme version of the scenario.

The report also analyses the implications of these direct and indirect consequences on insurance losses. The total of claims paid by the insurance industry is estimated at $21.4bn, rising to $71.1bn in the most extreme version of the scenario. One of the important considerations identified by this report for insurers is the wide range of claims that could be triggered by an attack on the US power grid, revealed in the matrix in Figure 4 at page 40.

The scenario in this report describes the actions of sophisticated attackers who are able to penetrate security as a result of detailed planning, technical skill and imagination. A relatively small team is able to achieve widespread impact, revealing one of the key exposure management challenges for insurers. However, the report also describes the constraints faced by the attackers, and shows that insurers should not believe this type of threat to be unlimited in its potential scope.

Claimant types

Insurance payments from the scenario would likely apply to six primary categories of claimant:

1. Power generation companies
- Property damage to their generators.
- Business interruption from being unable to sell electricity as a result of property damage.
- Incident response costs and fines from regulators for failing to provide power.

2. Defendant companies
- Companies sued by power generation businesses to recover a proportion of losses incurred under defendants' liability insurance.

3. Companies that lose power – companies that suffer losses as a result of the blackout.
- Property losses (principally to perishable cold store contents).
- Business interruption from power loss (with suppliers extension).
- Failure to protect workforces or causing pollution as a result of the loss of power.

4. Companies indirectly affected – a separate category of companies that are outside the power outage but are impacted by supply chain disruption emanating from the blackout region.
- Contingent business interruption and critical vendor coverage.
- Share price devaluation as a result of having inadequate contingency plans may generate claims under their directors' and officers' liability insurance.

5. Homeowners
- Property damage, principally resulting from fridge and freezer contents defrosting, covered by contents insurance.

6. Specialty
- Claims possible under various specialty covers, most importantly event cancellation.

Key findings

- Responding to these challenges will require innovation by insurers. The pace of innovation will likely be linked to the rate at which some of the uncertainties revealed in this report can be reduced.
- Cyber attack represents a peril that could trigger losses across multiple sectors of the economy.
- A key requirement for an insurance response to cyber risks will be to enhance the quality of data available and to continue the development of probabilistic modelling.
- The sharing of cyber attack data is a complex issue, but it could be an important element for enabling the insurance solutions required for this key emerging risk.

Conclusion

The cyber attack scenario in this report shows the broad range of claims that could be triggered by disruption to the US power grid. This poses a number of complex challenges for insurers, which would need to be addressed if insurers are to more accurately assess cyber risk and develop new cyber insurance products. Nevertheless, insurance has the potential to be a valuable tool for enhancing the management of, and resilience to, cyber risk.

Introduction to the scenario

The scenario was developed by the University of Cambridge Centre for Risk Studies and reflects a fictionalised account based on several historical and publically known real-world examples. The attack scenario was designed by subject matter experts and subjected to peer review to ensure that the effects could plausibly be achieved. In the interests of security, we have published only superficial details of the method of attack (which we have given the name the 'Erebos' Trojan).[4] This report does not reveal any previously unknown tactics or vulnerabilities.

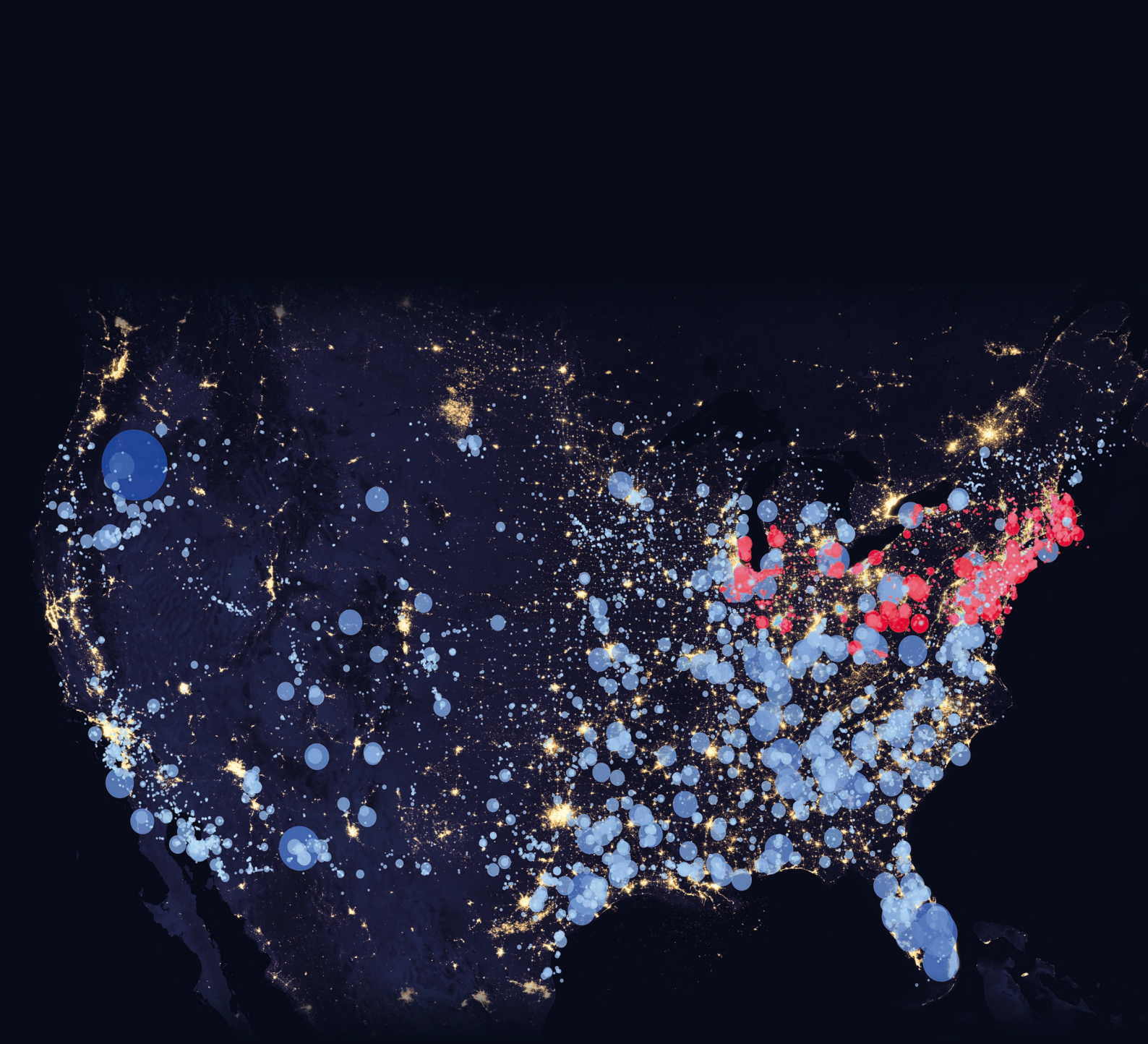
The Erebos Cyber Blackout Scenario is an extreme event and is not likely to occur. The report is not a prediction and it is not aimed at highlighting particular vulnerabilities in critical national infrastructure. Rather, the scenario is designed to challenge assumptions of practitioners in the insurance industry and highlight issues that may need addressing in order to be better prepared for these types of events.

By its design, the scenario that follows is intended to be useful and challenging for the insurance industry without defining a clear route to a real vulnerability for would-be attackers. It aims to bring awareness to the potential physical damage caused by cyber attacks against Operational Technology (OT), to make it a consideration for insurers in any cyber incident and, more importantly, to highlight potential insurance policy, legal, and aggregation issues in its analysis.

We have selected an event that highlights the complexity of insurance coverages in this area. We have tried to avoid proposing an event where the US Government would intervene to cover the insurers' costs through the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA 2015 or TRIA) or another backstop mechanism; the point of this report is to examine insurance coverages, rather than engage in debate regarding political interventions and policies.

Further detail on the methodology used to design the scenario is in Annex C to this report, and in Appendices 1 and 2, which accompany this report and are available online.

[4] *Erebos was a deity of Greek mythology, personifying darkness.*



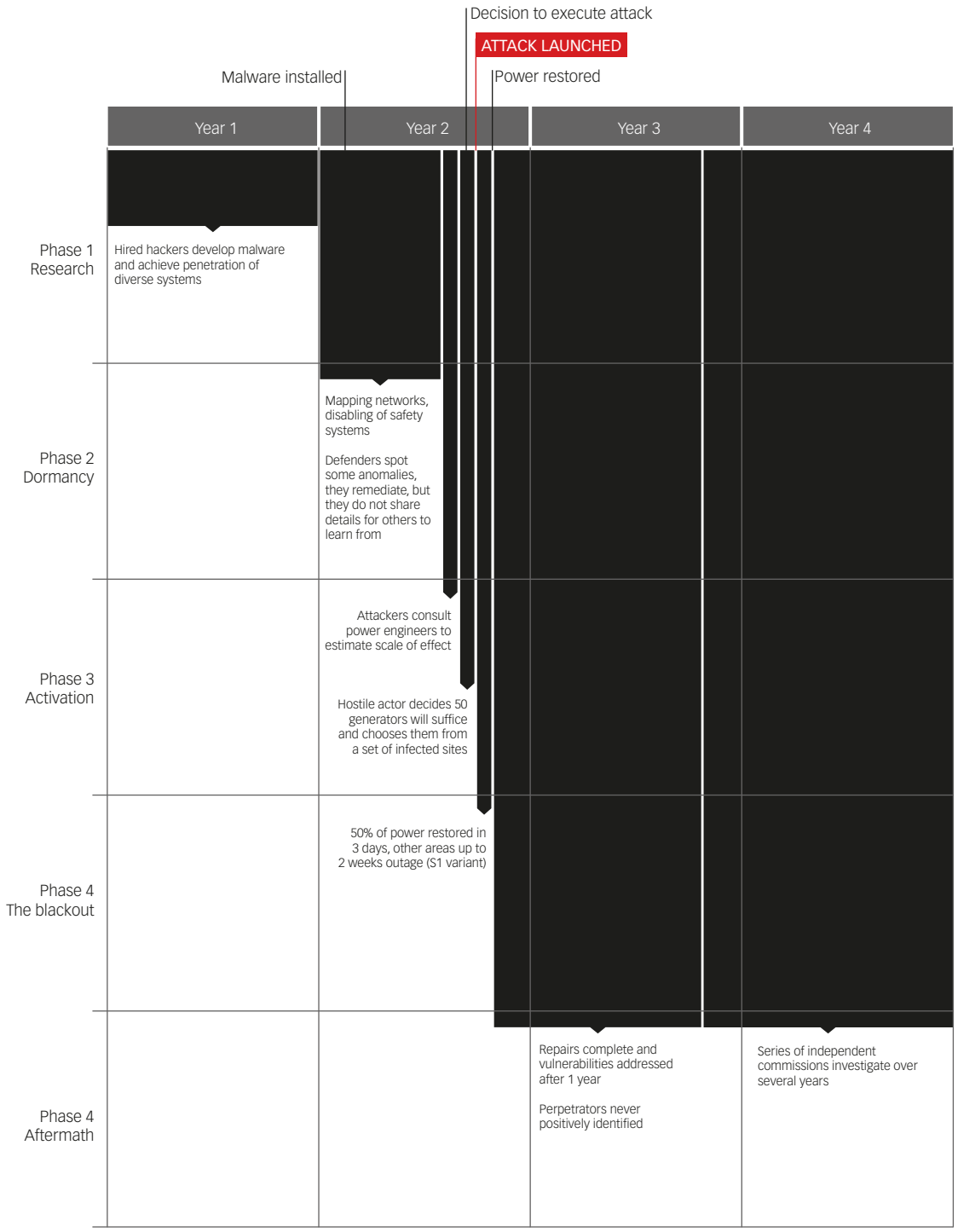
Erebos Cyber Blackout Scenario

This composite image depicts night lights in the continental USA (source: NASA Earth Observatory/NOAA NGDC) overlaid with the output capacity of power generation plants (Dataset: US Energy Information Administration, electricity power sales, revenue and energy efficiency Form EIA-861 detailed data files) and representations of 50 individual generators in the targeted region. It has been produced for illustrative purposes only.

Erebos Cyber Blackout Scenario

An unidentified group motivated to cause significant disruption inside the USA reaches out to the hacking community and purchases the services of a small group of morally dubious programmers who are knowledgeable of reverse engineering in the domestic electricity sector and grid systems. All of the hackers hired have very little idea of what they are working on as a collective.

Figure 1: Timeline of the Erebos Cyber Blackout Scenario



Phase 1: Research

The hackers spend months researching the US electricity markets, control systems and networks. They identify critical information flows, networks, devices and companies, and eventually begin writing a piece of malware designed to spread through generator control rooms without alerting system security teams.

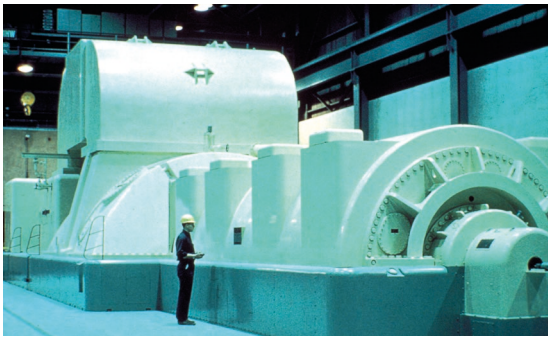
The team employs a range of tactics in their attempt to penetrate the security protecting the electrical grid. At least one of these methods is successful and they identify their preferred method of inserting malware into a number of target plant generator control rooms.

- Identification and targeting of laptops and other personal electronic devices used by key personnel with routine access to multiple power plants.
- 'Phishing' attacks designed to compromise the corporate network and pivot[5] into the control system.
- Hacking of remotely accessed control systems.
- Physical intrusion into locations used for network monitoring.

Phase 2: Dormancy

Once installed, the malware is able to 'call home' back to the programmers via the plants' network connections. It can now report information and receive commands from inside the network. The malware lies dormant. A second attack team monitors the 'dial out' connections from the malware's spread. This team is watching for signs that the malware has been detected, and monitors for a lengthy period to be satisfied that it has not been discovered.

A few power companies detect added traffic on their systems but do not identify it as a security threat, believing it is a fault or a vendor diagnostic connection. The infected machines are simply reimaged and no indicators of compromise are created. Reports of increased traffic are not shared between different companies owing to concerns about revealing vulnerabilities and protecting reputations.



Turbine generator. Source: wikipedia commons

Within the first 90 days, the attackers are able to assess the achievable range of control within the control room system. Chief among their observations is that, in roughly 10% of infection cases, they are able to access certain vulnerable generators.

A modern power station control room.

[5] *Once a machine is compromised, a hacker may be able to operate in the context of the machine itself and gain passage through a computer network by gaining access through other linked machines. This ability to establish chain attacks through multiple compromised machines is known as 'pivoting'.*

Phase 3: Activation

The attacker group begins performing packet captures, network scans and further exploitation to prepare for the day of action when the damaging events will be triggered. This is done by using Domain Name System (DNS) exfiltration as a command and control and by pivoting through the devices compromised by the initial malware infection. More than 100 sites are compromised but the protective relays make the attack non-viable at 57% of these control rooms, which are 'infected' but not damaged. This period of preparation for activation could take many months.

Despite only achieving a 10% success rate, the malware successfully infects over 70 generators by exploiting the systemic importance of control rooms, with each control room typically managing several generators.

The hostile actor decides to initiate the attack in July. The timing is driven in part by operational considerations, including the resource commitment to the project and the growing risk of discovery the longer the malware remains in place, and in part by analysis of electricity demand, which shows that an attack in the summer will cause widespread disruption. On the given day, the malware is activated and 50 generators are damaged in rapid succession.

The hackers covertly and systematically disable safety systems which would usually protect the generators from desynchronisation events. They send control signals which open and close the generator's rotating circuit breakers in quick succession, using the inertia of the generator itself to force the phase angle between supply and load out of sync. The impacted generators begin to catch fire and pour smoke; some are partially destroyed as the engine blows apart. One gas turbine facility is completely destroyed in an explosion resulting from the generator fire. Even undamaged generators across the region are shut down until the cause of the damage can be understood.

The Erebos Trojan causes critical damage to vulnerable generators, resulting in fire.

Phase 4: The blackout

The attack triggers a widespread blackout plunging 15 states and Washington DC into darkness and leaving 93 million people without power. It shuts down factories and commercial activity responsible for 32% of the country's economic production. Companies, hospitals and public facilities with backup generators are able to continue in operation, but all other activities requiring power are shut down. This includes phone systems, internet, television and radio, street lights, traffic signals, and many other facilities. Images of a dark New York City make front pages worldwide, accompanied by photographs of citizens stuck underground for hours on stranded subway cars and in elevators in the summer heat.

It quickly becomes clear that damage to 50 generators has caused the massive outage, though the reasons for the generator damage are not understood. An immediate coordinated effort is made to restore power and, within three days, roughly half of the affected area is successfully put back on supply. Nevertheless, high demand regions continue to suffer rolling blackouts for weeks while electricity companies work to repair power distribution.

Some areas, including parts of New York City, remain without power for up to two weeks. This is caused by uncertainty over the reasons for the damage suffered by generators. Affected utility companies are reluctant to synchronise their facilities to the bulk power system until they understand what caused the generator damage. The risk of permanent damage to generators is assessed to be greater than the cost of lost revenue from being offline while the problem is being investigated.

Phase 5: Aftermath

As the power finally returns to the last affected areas, the national media begins to seek an explanation. In a report to Congress, a speaker for the US Department of Energy reveals that internal investigations have found a piece of culpable malware – the virus 'Erebos'[6] – in a handful of generation rooms in the Northeastern United States region and are conducting a thorough investigation to uncover the spread of the infection. The media christens the mass blackout as the "Erebos Event".

In this post-damage period, efforts are made to understand both the malware and its range of infection. The process of reverse engineering the malware is time

Manhattan blackout.

consuming. The engineers have difficulty providing definitive answers to their executive boards about the risk of connecting generators to the bulk electrical system as they do not know what other sites, devices, files and networks may be compromised or infected. Computer scientists and electrical engineers collaborate to investigate and confirm the scope of the infection across multiple sites. The electrical engineers understand how damage has occurred and how to prevent it but do not understand which sites, devices, files and networks are compromised.

Political pressure builds for the US Government to assign responsibility for the attack, but it is difficult to do so unequivocally as the complex attack must be fully understood before it can be properly traced. Political leaders and officials want to understand the nature of the attack in order to accurately assess the threat before they can consider action against any suspected perpetrators.

Eventually, the contagion is traced back to the original site of infection and the malware is better understood. The timeline of infection at various sites is reconstructed and it becomes possible for investigators to locate and trace the command-and-control servers used in the attack. After a brief international search and law enforcement reciprocation negotiations, the servers are identified in a number of foreign countries. The governments of those countries allow them to be forensically imaged and removed from service. The servers, which have been abandoned, provide no clues to the identity of the perpetrators. Reverse engineering and forensic examination of these machines allows the identification of further infected control rooms which, although not damaged in the attack, remain vulnerable to compromise.

The process of revealing the full scope of the infection and repairing the damaged cyber and physical systems is accomplished over the course of the following year. Several national independent commissions are established to investigate different aspects of the incident, and the ramifications of the attack continue to be felt for many years afterwards.

Direct impacts on the economy

Approximately 50 generators that supply power to the Northeastern United States are damaged by the malware. The generators are taken offline as soon as they are damaged, and, since some of these generators provide base load to the region, this process causes an initial power outage. As the number of generators taken offline increases, the grid destabilises. This causes a temporary frequency response event which further exaggerates the blackout on the wider grid by causing a cascading outage across the NPCC and RFC[6] region, similar to the 2003 Northwest Cascading Power Failure. Other generators in the region that are not affected by the malware switch into 'safe mode' due to the destabilised grid and disconnect from the power network in an effort to prevent damage from an overload.

Power is restored to some areas in an average of three days but other places remain in the dark or with rolling blackouts for weeks. Our modelling does not predict which areas will be reconnected in which order. Our overall estimate of the pace of reconnection shows the overall percentage of the population that is back on power, but the localised pattern of where the restoration will occur is not predictable.

The following chart and table summarise the length of the outages in each variant scenario. The area beneath the restoration curves in the chart represent 'City-Days' spent without power. Though the blackout is widespread and long-lasting in the standard variant (S1 and S2) and extreme (X1) scenarios, the effect of the generator damage and reparations on supply means that not all

Figure 2: Duration and extent of power outages for each scenario variant

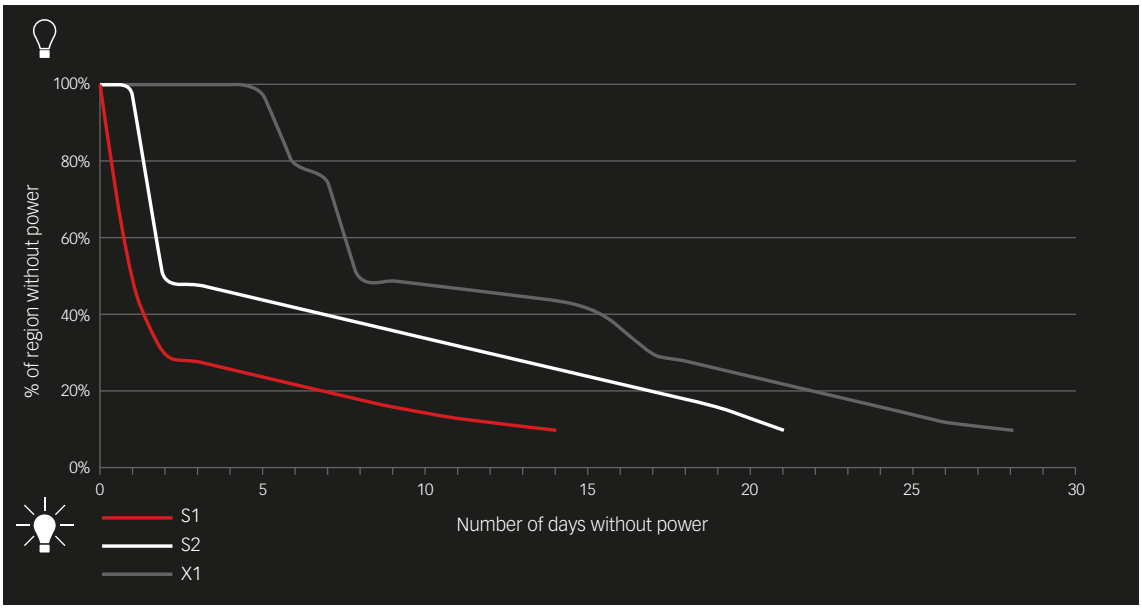


Table 1: Severity of impacts for each scenario variant

Scenario	Outage duration, weeks (to 90% restoration)	City-Days	Number of damaged generators	Percentage of generators vulnerable to contagion
S1	2	3.78	50	10%
S2	3	8.08	50	10%
X1	4	13.83	100	20%

[6] The Northeast Power Co-ordination Council (NPCC) and ReliabilityFirst Corporation (RFC) are regional electric reliability councils which aim to ensure the reliability of the bulk power system in the region covered by the scenario. See Annex B for further details.

customers in the area are without power. The City-Days metric helps approximate the additive period spent completely without power in the region. Further detail on the methodology used to generate these projections is in Appendix 2 (available online).

Primary effects

Health and safety

Although only a few people are hurt in the initial incident, the long power outage does take its toll in human deaths and injury. There are many accidents resulting from the blackout, including road traffic and industrial accidents. There are people hurt in riots, looting and arson attacks. As the power cuts continue through the hot summer months, heat stress affects older and infirm people, with a rash of deaths reported in nursing homes. Backup generator failures in hospitals result in treatment equipment failing. People are reported sick from eating food that has defrosted or not been properly cooked.

In some cases industrial accidents cause environmental damage, and water treatment failures result in pollution to water courses.

Productivity

The power outage causes a decrease in business productivity as workplaces close and people are unable to get to work. Although some manufacturing and commercial facilities have backup generators, these typically provide only partial replacement. While some workers may be able to perform duties even without electricity many, particularly in the cities, are unable to get to their place of employment due to the wider disruptive impact of the blackout on public transportation and fuel stations. Productivity remains low, therefore, even as some businesses are returned to power.

Trade

Maritime port operations are suspended during the power outage. Loading and unloading container ships becomes impossible without electricity, and import and export activity is interrupted. Goods for export that do make it to the port are backed up awaiting the resumption of port activities, prompting a halt in production and a cascading impact along the supply chain as demand for inputs into production processes are temporarily curtailed. Any economic activity relying on imports for production is also disrupted.

Consumption

Although the first day of the outage sees an upturn in the rate of consumption due to panic buying, this effect is quickly overtaken by the far more disruptive impact of the failure of electronic methods of payment. Cash quickly becomes the only accepted form of payment

Workplaces close as people are unable to get to work.

Loading and unloading container ships becomes impossible.

but the shortage of serviceable ATMs means that many citizens are unable to obtain paper money. Consumption levels remain low until all affected customers are returned to power.

Water supply
Water supplies are impacted during the blackout due to the loss of power to pumps. Supplies of potable water become limited across the affected area.

A week into the outage, it is revealed that a chemical plant accidentally allowed a dangerous compound to enter the local water supply due to lack of power and a broken backup generator. This causes a localised bout of sickness involving 10,000 people being treated for moderate to serious symptoms.

Several accidental spills occur from sewage plants suffering power outages, leading to further contamination of the water supply serving 2 million people in a different part of the region. Malfunctioning and overflowing sanitary systems force many businesses to shut down due to health concerns.

Transportation
Traffic signals cease functioning as soon as the blackout hits leading to a sharp spike in road accidents and gridlock. There is a run on vehicle fuel and a rapid reduction in the number of operational fuel stations. The majority of people stop using their cars.

All electric locomotive railroad services are non-operational during the crisis. City subways are taken offline during the outage and replacement bus services are provided.

Regional airports are shut down due to lack of power for security screening equipment. All major airports serving New York City and Washington DC are also closed for the first day of the outage due to the lack of electronic ticket verification, constituting a serious security risk. They reopen the next day but spend another week dealing with the chaos caused by the power outage.

Communication
All forms of communication systems without backup power supplies are hampered by electricity failure. Telephone communication circuits are initially overloaded, making it extremely difficult to make calls. Mobile phone data and service providers remain in operation for several hours after the initial outage but begin to shut down as their backup batteries fail and generators run out of fuel. The backup diesel generators for emergency services keep 911 online, but the loss in communication means that, for most, the service is unavailable. Internet service also fails. Over-the-air TV remains broadcast in some areas but few have power to receive it. Emergency radio and word-of-mouth are the primary means for people to receive information.

Information and communication technology (ICT) is a core activity and a significant contributor to value-added in the economy. All sectors rely on some form of ICT, particularly finance, services and retail. Most sectors depend on electronic financial transactions, email and the internet for commercial activity. None of these systems work in the event of electricity failure, forcing these businesses to either shut down or find alternative methods of communication. Communication failure makes it very difficult for response agencies to know what areas have been impacted and where to prioritise resources, slowing the recovery and prolonging economic disruption.

Tourism
The outage has a serious impact on tourism as airports and rail services are shut down. Tourists are unable to get to their destinations and abandon their travel plans. Spending by tourists is severely reduced for the duration of the outage and does not return to normal levels until several weeks after power is fully restored.

Secondary effects

Outbreaks of looting and stealing occur as the outage drags on, with criminals exploiting the lack of lighting and security systems coupled with overstretched police forces. Looting intensifies as people run low on food and water in the hot summer and become increasingly frustrated. By the second week without power, many communities suffer a general sense of social unrest, with many people choosing not to go out after dark.

As the power outage continues to deny basic services, social unrest increases. Health and safety suffers owing to factors such as contaminated water and food supplies, difficulties in using at-home healthcare equipment or securing repeat prescriptions, added noise and air pollution from generators, increased physical exertion and poor emergency response. These factors all contribute to a higher death rate in periods of power outage.[7]

Mobile phone service suppliers begin to shut down as backup systems fail.

[7] *Klinger et al., 2014.*

Long term effects

Suspicion for the attack is focused on a small number of nation states believed to be hostile to the USA, citing a variety of motives, but the subsequent investigation does not establish any proof of direct involvement. As a result, litigation is pursued by a wide range of parties, lasting several years. The incident has a significant impact on safety and security in the power generation sector in the USA and around the world. New regulations require the redesign of certain aspects of the power grid Information Technology/Operational Technology (IT/OT) architecture. Data sharing on cyber attacks increases substantially in all sectors, especially in power and critical infrastructure industries.

Macroeconomic analysis

Introduction

Modern economic activity depends on the availability of electricity, and any significant interruption to electricity supply has severe economic consequences. Growing demand means the USA is becoming ever more dependent on power for economic growth, placing an increasing strain on ageing electricity networks. These trends are driven by the growth in electricity intensive industries such as energy and manufacturing and a new demand for consumer electronics and ICT. The rapid pace of change and the increasing interdependency between different sectors of the economy means that it is difficult to fully predict how different technical, social and economic systems will react to large power system failure; further detail on the methodology used to generate the estimates of economic loss is given in the accompanying Appendix 2 (available online).

Evidence from historical outages and indicative modelling suggests that power interruptions already cost the US economy roughly $96bn[8] annually.[9] However, uncertainty and sensitivity analysis suggest this figure may range from $36bn to $156bn. Currently over 95% of outage costs are borne by the commercial and industrial sectors due to the high dependence on electricity as an input factor of production.[10] The majority of these costs (67%) are from short interruptions lasting five minutes or less.[11] This estimate only provides the expected annual economic loss in an average year, and does not give an indication for the losses that might occur due to a single extreme event.

Categories of economic loss

The economic losses from electricity failure can be broken down as follows:

Direct damage to assets and infrastructure: the costs associated with replacing damaged assets, when this is the cause of electricity failure.

Direct loss in sales revenue to electricity supply companies: the revenue that would have been generated if the power failure had not occurred. Estimating revenue losses is achieved by multiplying the expected price of electricity by the amount of electricity that would have been supplied in the event of no failure. Lost revenue would impact generator companies, electricity supply companies and network operators.

Direct loss in sales revenue to business: the revenue that a business would have received if the supply of electricity had not failed. This is the integrated difference between the projected 'no disaster' trajectory and the trajectory defined by the scenario where electricity fails. This value varies greatly by sector and from one business to the next, largely depending on their reliance on an electricity supply under normal operating conditions and the availability of backup electricity supply systems.

The estimates for revenue at risk for electricity supply companies and the wider business sector are detailed in Table 2 below.

Indirect losses through value chains: the losses upstream and downstream caused by direct interruption to production activities. The lack of supply of electricity prevents goods and services being produced and leads to losses both up and downstream in the supply chain.

Long term economic effects: changes in the behaviour of market participants as a result of perceived long-term changes in supply security, including the choice of business location, potential increase in prices due to an increased need for backup facilities and customer churn from unreliable delivery deadlines.

Different classes of customer will experience different losses within these categories. At a broad level, these can be broken down into residential, commercial and industrial customers.

Table 2: Lost power supply and revenue impacts under each scenario variant

Scenario variants	Lost power at peak-hour capacity (TWh)	Lost power at average capacity (TWh)	Electricity Revenue@Risk	Sector Losses Direct Revenue@Risk	GDP@Risk (5 Yr)
S1	9.9	7.2	$1.15bn	$60.9bn	$243bn
S2	36.9	21.0	$2.46bn	$130.2bn	$544bn
X1	63.1	36.0	$4.21bn	$222.8bn	$1,024bn

[8] Based on data given in US$ 2004 constant prices and converted to US$ 2015 prices using the GDP deflator for the period 2004–2015 estimated to be 1.2.

[9] K. LaCommare and J. Eto, "Understanding the Cost of Power Interruptions to US Electrical Consumers", University of California Berkeley, September 2004.

[10] The economic losses can be split into commercial (72%), industrial (26%) and residential (2%) sectors.

[11] LaCommare & Eto, ibid.

The residential sector In the electricity regions targeted in this scenario (the NPCC and RFC regions, as described at Annex C), the residential sector consumes 36% of all electricity but across all sectors incurs the smallest cost per unit of unsupplied electricity. This is because the electricity delivered to households is considered as final consumption, ie it is not used to produce goods for use as inputs elsewhere in the economy. Households are not considered to use electricity to generate income, so losses are the direct costs incurred by undelivered electricity. Losses can be grouped into material and immaterial losses. Material costs include out-of-pocket expenses such as candles, prepared food and food spoilage. Immaterial losses include stress, inconvenience, fear and anxiety, etc. Immaterial losses are particularly difficult to evaluate but can be captured using contingent valuation techniques where people are asked how much they would be willing to pay to avoid an electricity outage or, alternatively, how much they would be willing to accept as payment to experience an outage.

The industrial sector incurs the highest direct and indirect losses for unsupplied electricity. In 2014, the industrial sector accounted for 25% of total electricity consumption within NPCC and RFC. Electricity is required as an input factor of production to produce goods that are used elsewhere in the economy, meaning that the impacts compound along the supply chain. This is particularly important for supply chains that operate using 'just-in-time' philosophy and therefore have little inventory to draw on. In an outage event with a long duration, even industries with large stocks of inventory may experience supply chain disruption. Several studies have estimated the value of lost load to industrial customers as being in the range of US$10 and US$50 for each kWh of electricity unserved[12].

The commercial sector consumes 39% of total electricity and as a sector is willing to pay twice as much as the industrial sector on average to avoid a power outage[13]. This is most likely explained by the commercial sector's high dependence on electricity for making sales and a loss of patronage and reputation in the event of electricity failure. Unlike the industrial sector, the commercial sector sells most of its goods directly to end consumers, thus downstream indirect losses are capped. However, as the commercial sector purchases its goods from elsewhere in the economy, upstream indirect losses will be significant.

Impact by economic sector

Table 3 below provides the estimated losses for each sector of the economy under the scenario variants.

The estimates were generated using a methodology developed by Reichl et al (2013) for estimating the direct dollar value of lost electricity load across different sectors of the economy.

Table 3: Economic cost of the Erebos event by sector and scenario variant

Cost of electricity interruption ($bn)	S1	S2	X1
Wholesale and retail trade	$14.35	$30.68	$52.51
Public sector	$8.53	$18.24	$31.22
Households	$7.54	$16.12	$27.60
Manufacturing	$6.41	$13.71	$23.46
Accommodation and food services	$5.64	$12.05	$20.62
Administrative support services	$4.65	$9.95	$17.02
Professional, scientific and technical services	$4.19	$8.96	$15.34
Real estate	$3.62	$7.74	$13.24
Information and communication	$1.86	$3.97	$6.80
Finance and insurance	$1.77	$3.78	$6.47
Transport	$0.63	$1.34	$2.29
Agriculture	$0.62	$1.32	$2.26
Electricity and gas supply	$0.45	$0.96	$1.65
Construction	$0.37	$0.78	$1.34
Mining	$0.20	$0.44	$0.75
Water supply, waste management	$0.07	$0.15	$0.26
Total	$60.90	$130.19	$222.83

Impact to the US economy

The economy suffers both supply and demand side shocks. On the demand side, consumption is impacted because people are unable to complete economic transactions, are not able to travel to buy goods and cannot use online sources to make purchases. Exports and imports are also impacted, as ports are not able to load and unload goods that come from international markets. On the supply side, labour is negatively impacted because people are either unable to get to work or their productivity is critically dependent on electrically powered technology. All of these factors have serious negative consequences on market confidence.

For the areas affected by electricity failure, it is assumed that there is a 100% shock to exports and a 50% drop in labour productivity and consumption for the duration of the outage in each variant of the scenario. For example, in S1 the regions affected represent 29.5% of the US population for 3.78 outage days. Over one quarter this represents a shock to the US economy of 0.61%. This process was repeated for each of the variants and each of the variables being shocked. These values are given in Table 4.

[12] *Eto et al., 2001; Reichl 2013; Royal Academy of Engineers, 2014.*

[13] *Reichl et al., 2013.*

Table 4: Macroeconomic shocks applied to the Oxford Economics Model

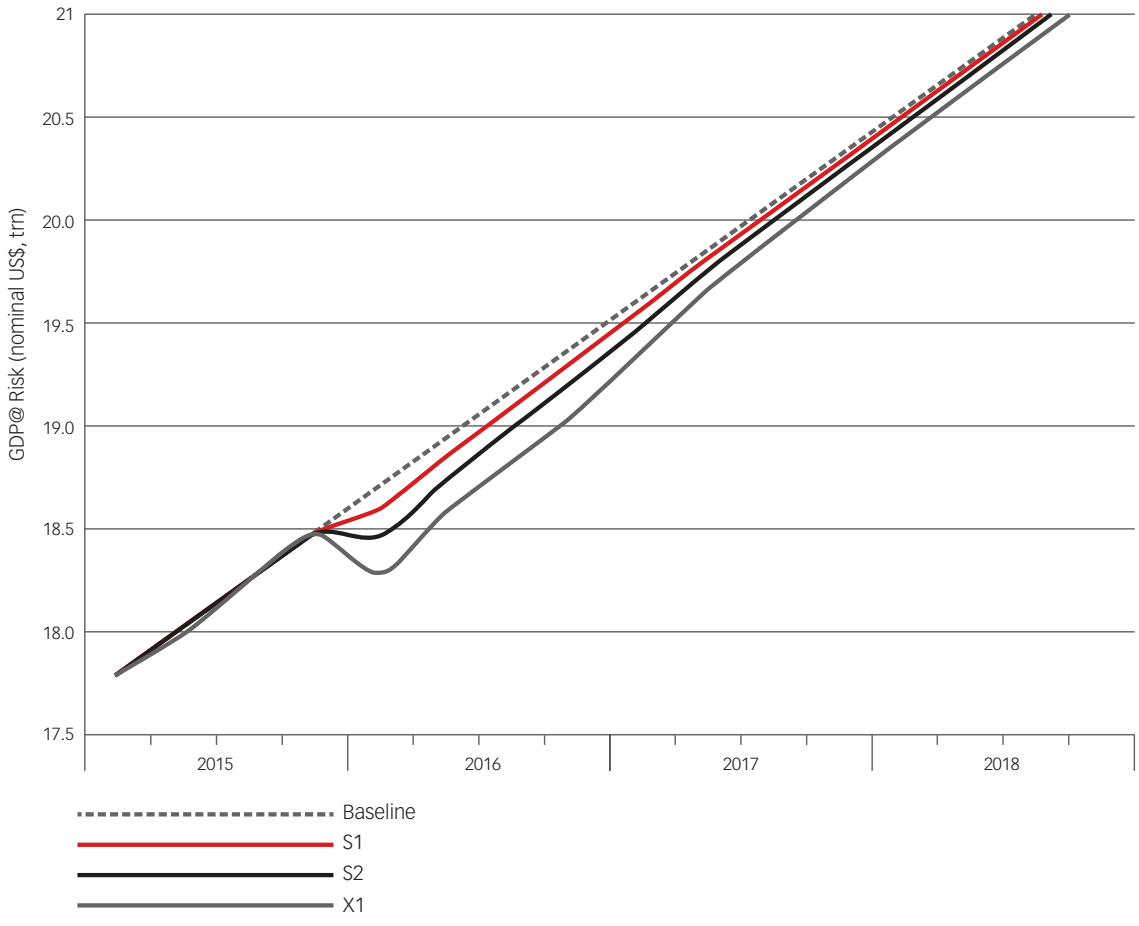
	Duration	Consumption	Labour	Exports	Confidence
S1	2 weeks	0.61%	0.61%	1.32%	-5%
S2	3 weeks	1.31%	1.31%	2.84%	-10%
X1	4 weeks	2.24%	2.24%	4.85%	-20%

By applying these shocks to the Oxford Economics Model we are able to derive estimates for the total USA 'GDP@Risk' under each scenario variant.

The GDP@Risk for the USA is shown in Figure 3. These results suggest that although the initial shock on the economy is severe, it reverts to pre-shock equilibrium levels before the end of the third year. In the standard variant scenario, when the crisis lasts two weeks to 90% power restoration, the total expected GDP@Risk is £243bn. At the other extreme, in the X1 scenario the outage lasts four weeks and the losses to the economy exceed $1trn.

Note that the economic impacts are non-linear with respect to the size and duration of the outage. Even though the marginal cost of electricity failure decreases for direct losses, the reverse is true for indirect losses. The marginal cost of indirect losses grows as the severity of the outage increases and the duration is extended across scenario variants. The economy is slow to rebound to pre-disaster levels once power is returned. For extended outages like in X1, businesses may relocate to other regions, market confidence will wane for several quarters, international competitiveness will drop, and investments from overseas will be diverted elsewhere. The relationship between direct and indirect impacts concurs with the existing literature, which suggests indirect impacts are of much larger magnitude than direct impacts.

Figure 3: Domestic USA GDP@Risk under each variant of the Erebos Cyber Blackout Scenario



Cyber as an emerging insurance risk

Cyber insurance is a rapidly growing market and London has become a centre of expertise and capacity for this new form of risk. Corporate risk managers see cyber attacks as one of their most serious concerns and obtaining cyber insurance protection is becoming an increasingly important part of business risk management. Most corporations are experiencing frequent cyber attacks and attempted compromises of their IT systems, so they are aware that the threat is significant.

The characteristics of cyber risk

Cyber is an unusual insurance risk. It is a relatively young phenomenon and so there is only a short history of claims experience available to calibrate the likelihood of future risk.

While there have been large individual business losses attributed to cyber attacks there have so far been no examples of catastrophe-level losses from a widespread cyber attack having a severe impact on many companies all at once.

It is a dynamic risk – the technology applications, software vulnerabilities, preferred attack practices by perpetrators, legal case law and compensation practices, and insurance product design and coverage offerings, are all rapidly changing.

Insurers are also realising that the cyber threat has the potential to generate claims from lines of insured business where cyber damage is not an explicit cover. This 'silent' cyber exposure refers to instances where claims may arise under an all risks cover. Insurers may not realise the extent of their exposure to this emerging threat class, and may not have charged premium to cover this aspect of the risk. Insurers may be holding more cyber exposure in unexpected lines of business in their portfolio than they realise.

The greatest concern for insurers, however, is that the risk itself is not constrained by the conventional boundaries of geography, jurisdiction or physical laws. The scalability of cyber attacks – the potential for systemic events that could simultaneously impact large numbers of companies – is a major concern for participants in the cyber insurance market who are amassing large numbers of accounts in their cyber insurance portfolio. The common perception of cyber threat is that a few lines of malicious code can be written fairly easily to infect systems widely and indiscriminately across the entire internet[14] – huge improvements in security by corporate systems have not fully alleviated the fear of widespread and systemic attack. Insurance companies cite their poor understanding of their probable maximum loss (PML) as one of the main reasons for not making more capacity available to meet demand for cyber insurance.[15]

However, cyber attacks and IT events are not unlimited or infinitely scalable. They can have significant constraints that limit attack severity and curtail the amount of loss that insurers may face. A successful cyber attack has to overcome all the security systems put into place to protect against it, requires expertise and resources by the perpetrators who face their own risks of identification, prosecution and retribution, and the loss consequences of attacks are mitigated by risk management actions. Further discussion of these factors is in Annex C.

Cyber insurance

Cyber attacks trigger different insurance policies depending on the targeted system and damages incurred. An Information Technology (IT) attack, such as a data breach, may activate data breach, data loss or data recovery policies. However, an Operational Technology (OT) attack, such as an attack on a manufacturing plant, may activate both first and third party business interruption policies as well as property damage policies if physical damage occurs.

On occasion, IT and OT cyber attacks are also covered by affirmative cyber policies. In some situations OT cyber attacks may be covered by traditional general liability policies. There is also a difference in insurance policy interpretation of traditional liability policies; some insurers remain silent while others offer affirmative cyber coverage. If the insurers are silent on the issue, then it is open to interpretation whether or not the general policy covers certain cyber events.

[14] *Notorious examples like the iloveyou computer worm that attacked tens of millions of Windows personal computers in 2000 were powerful precedents that suggested mass scaling attacks would be serious problems for businesses. Fortunately new generations of security systems provide greatly improved protection against unsophisticated malware.*

[15] *HM Government UK and Marsh Ltd. (2015)*

Challenges for the development of cyber cover

The current cyber insurance market is dominated by IT policies; OT cyber policies are less common. IT-related cyber attacks, such as high profile data breaches, have been widely reported, while OT attacks have received less publicity. Examples of historical OT attacks with insurance payouts and demonstrable economic damage are less common. This presents a challenge for the process of creating pertinent insurance cover. Members of the critical national infrastructure industry in particular are increasingly at risk of both IT and OT cyber attacks, and could potentially benefit from insurance coverage for both.

Given the evolving threat landscape of cyber risk, particularly in the OT event domain, insurers need to assess cyber risk technically rather than statistically. The Chief Risk Officers' (CRO) Forum has outlined four specific challenges that the insurance market faces in its endeavour to properly assess cyber risk[16].

- Insufficient or poor quality loss information – available historical data does not reflect the current environment or evolving threat landscape.
- Uncertain value of loss information - there is no established calculation method and poor information sharing.
- Highly interconnected IT systems – it is hard to measure an insurer's cyber risk exposure accumulation.
- Continually evolving attack strategies, perpetrators and motives – only motive and attribution for an attack will determine whether clauses and exclusions can be considered.

These challenges highlight the need for collective approaches to sharing data, particularly overcoming the reluctance to disclose information to other risk stakeholders, and most importantly, carrying out analysis of potential scenarios of future cyber risk events.

[16] *CRO Forum, 2014.*

Insurance industry loss estimation

Insurers would see a large number of claims resulting from this scenario, across many lines of business. In this section, we estimate the losses that the insurance industry would be likely to pay out. Table 5 shows the losses for the main areas of insurance business that are likely to drive the total payouts. A detailed breakdown of estimated losses by line of insurance is at Figure 4. We describe the main assumptions in this section.

We also provide a guide for calculating an insurance company's portfolio-specific loss that would be compatible with this scenario – this is available online with this report.

Claimant types

The loss would be expected to derive predominantly from six categories of claimant:

1. **Power generation companies** – the companies that own the generators and use them to generate and sell electrical power to the grid. They suffer property damage (to their generators), business interruption in being unable to sell electricity as a result of property damage, together with incident response costs and fines from the regulators for failing to provide power.

2. **Defendant companies** – companies sued by the power generation firms to recover some of their losses. Defendant companies are likely to be different types of organisations who provided the generators and control systems that proved vulnerable to the attack. Litigation costs and settlements are claimed under the defendants' liability insurance. These defendant companies include: engineering companies that manufactured and supplied the vulnerable generators; suppliers of control room systems; developers of the control system software; developers of the security software providing firewalls and malware protection; and, any companies involved in the 'vector' of introducing the malware into the control rooms.

3. **Companies that lose power** – companies that suffer losses as a result of the blackout. These include those that are in the areas of the outage and that suffer property losses (principally to perishable cold store contents) and those who have insurance coverage with suppliers extension to pay out on business interruption from power loss. Any company that fails to protect its workforce, or that causes a polluting accident resulting from the outage, or is adversely impacted by the event and suffers disproportionately, particularly as a result of management decisions, may also generate claims under various coverages in their liability insurance.

4. **Companies indirectly affected** – A separate category of companies are those outside the area of the outage but that are impacted by a company in the blackout

Table 5: Estimated insurance industry losses resulting from the three variants of the scenario ($m)

		Scenario variant		
CLAIMANT TYPE	COVERAGE	S1	S2	X1
Power generation companies				
	Property damage (generators)	633	835	1,569
	Business interruption (generator damage)	3,817	5,499	11,462
	Incident response costs	3	5	4
	Fines – FERC/NERC[17]	4	8	18
Defendant companies				
	Liabilility	2,253	2,363	3,196
Companies that lose power				
	Perishable contents	595	711	901
	Contingent business interruption – suppliers extension	6,769	15,668	25,452
	Liability	3,120	6,240	12,480
Companies indirectly affected				
	Contingent business interruption – Critical vendor	2,928	6,542	12,318
	Liability (D&O)	749	1,498	2,995
Homeowners				
	Household contents	465	465	465
Specialty				
	Event cancellation	63	126	252
TOTAL		21,398	39,957	71,109

[17] *Federal Energy Regulatory Commission (FERC), North American Electric Reliability Council (NERC).*

Table 6: Values and deductibles assumed for power generation company claims under property and business interruption insurance

Generator size	Approximate MW	Approximate asset value, $m	Approximate deductible, $m	Business interruption days	Limit, $m
Large	1000 MW	$50	$1.00	60	$50
Medium	500 MW	$30	$0.50	45	$50
Small	100 MW	$1	$0.25	14	$50

region which provides them with vital supplies and that claim contingent business interruption critical vendor coverage. Companies that suffer share price devaluation as a result of having inadequate contingency plans may generate claims under their directors' and officers' liability insurance.

5. **Homeowners** – individual households suffering power losses may file claims for any property damage, principally resulting from fridge and freezer contents defrosting, covered by their contents insurance.

6. **Specialty** – the power outage is likely to cause claims under various specialty covers, most importantly event cancellation.

Power generation companies

Property loss

There are around 150 companies that generate power in the zones of NPCC and RFC, operating 261 power plants that contain 676 generators with capacities of over 100 MW. The S1 and S2 scenario variants envision 50 of these generators – around 7% of the total – being damaged. In X1 it is 100 generators – 14%. In the scenario, we have not specified which generators these are, but have modelled a range of permutations of damaged generators in different companies and plants. In variant S1, each suffers loss of around 30% of its total value in damage although at least one suffers an explosion and is a total loss. In variant S2 the damage ratio is 40% and in X1 the damage ratio is 50%. The buildings surrounding the generators and other equipment suffer minor damage.

The loss from this property damage is claimed from insurers by the power companies under their property insurance, and any affirmative cyber insurance policies that include property loss. We have assumed that all of the damaged generators are insured, at an average value of $107,500 per MW of capacity.[18]

Table 6 shows the assumptions made about deductibles and limits applied to the generators in the insurance programmes of the power generating companies.

Business interruption

The damage to the generators prevents the power generation companies from generating and selling power to the grid while the generators are repaired and brought back online. They claim for this loss under their business interruption coverage on their property insurance. A monthly rate of loss of $83,000 per MW lost is assumed equivalent to the average value of the power sold by the company to the market. Deductibles and limits assumed are provided in Table 7. Repair times for generators are derived from estimates of repairing different severities and mechanisms of damage, for example replacing burnt-out bushings, reconditioning broken crank shafts, and ordering and installing new replacement generators where totally destroyed.

Table 7: Summary of power company business interruption values

	S1	S2	X1
Average months out of service	3.5	4.5	5.5
Deductible max. limit, months	6	6	6

Incident response costs

The incident will generate additional costs for the power generation companies in their emergency response to the event, the clean-up and making safe processes, and post-event investigation and forensics. The technical response will include the making safe of the malware, ensuring the system is clear of any similar threats, and investigation of the provenance of the malware and the vectors and vulnerabilities exploited in infecting the system to prevent any recurrence. These incident response costs will be claimed under the property insurance policies, and any cyber affirmative covers purchased. Costs of upgrading the system to a more secure standard are not recoverable under most standard cyber insurance policies. We expect these incident response costs to be mainly internal staff costs but these may involve external consultants with relevant skills working for several weeks on site at billable rates.

[18] *Hynes, 2009.*

Power generation companies that do not suffer damage are also likely to carry out internal system checks to see if they are infected with the malware and to identify any vulnerabilities that could cause them similar problems in the future. These companies may be able to recover some of their costs under cyber insurance policies, depending on the coverage structures.

Fines

The power generation companies face civil penalty fines from their regulators for failing to meet key security and reliability standards. Fines can be levied by the Federal Energy Regulatory Commission (FERC) based on North American Electric Reliability Corporation (NERC) standards. Fines of up to $25m have been levied on power companies, and we have assumed that fines levied would be similar to those resulting from previous precedent outages, and scaled according to the loss (see breakout box).

FERC fines

NERC maintains reliability standards over its associated industries, which include critical infrastructure protection (CIP) security standards. NERC conducts annual audits of various electric utilities over the course of the year, either randomly or after a major outage event.

The Federal Energy Regulatory Commission (FERC) can then impose fines on electricity companies for violating these NERC reliability and CIP standards and can be as high as $1m per day. (Tripwire) The CIP fines focus in particular on cyber security standards.

Typically, a portion of these fines is paid to the US Treasury and NERC, while the remainder is used by the electricity company to make improvements in keeping with reliability and security standards.

Although civil penalty fines for violation of NERC reliability standards typically range from $50,000 to $350,000, there are recent examples of fines greater than $1m, especially in cases where an outage has occurred. (DeJesus and Halpern, 2013)

- Florida Power and Light Company (FPL) was made to pay a $25m fine for violating reliability standards in 2009. (DeJesus and Halpern, 2013)
- PacifiCorp was required to pay $3.925m for a 2011 outage. (DeJesus and Halpern, 2013)
- Arizona Public Service Company (APS) was forced to pay $3.25m in fines for the 2011 Southwest outage that affected 5 million people. (Peace and Tweed, 2014)

There is also a precedent of FERC fining an entire NERC region. A 2008 outage in the Florida Reliability Coordinating Council (FRCC) left almost one million people without power and FRCC was made to pay a $350,000 fine. (Daly, 2010)

In addition, legal sanctions could be imposed by the Attorneys General of states that are affected, and potentially by the federal government. Some of these regulatory fines may be recoverable under insurance coverages.

Other liabilities

Companies that operate under 'Common Carriage' (eg energy companies, telecoms, transport, public utility companies) have tariff protection from their regulator to protect them from legal action from their customers. These protections have been frequently tested in law suits but have proven resilient.

Power generation companies do purchase liability insurance, but we assume that although there may well be legal cases arising, the tariff protection will continue to hold, and that insurance payouts under liability covers for the power generation companies will be minimal.

Defendant companies

We assume that the power generation companies sue a number of their suppliers who they claim are culpable in the security failure to protect their systems from the malware and in the vulnerability of the generators to cyber attack. They claim the net losses that they suffer that they have not been able to recover from their insurers or others, including non-insured assets, exclusions, co-insurance deductibles, and losses above policy limits.

Defendant companies could include:

- Engineering companies that manufactured, installed, and maintained the vulnerable generators.
- Suppliers of control room systems.
- Developers of the control system software.
- Developers of the security software providing firewalls and malware protection.
- Any companies involved in the 'vector' of introducing the malware into the control rooms.

Liability loss assumptions

We assume that these defendant companies carry liability insurance and that claims are aligned with errors and omissions and other liability coverages. The insurers of each of these defendant companies take control of the litigation as soon as they are notified of the suit. The chain of liability is complicated by the fact that no individual company is solely responsible, but the cyber attack could only have succeeded with several of the vulnerabilities and defects in combination. We assume that the power generation companies are broadly successful and recover around 90% of their claim. Software companies offer a defence that they have

Legal ambiguities in power outage claims

Historically, mass torts against power companies for failure to supply electricity resulting in property damage have not gone favourably for the plaintiffs. The burden of proof of gross negligence is placed on the plaintiff to prove that significant property damage or personal injury occurred as a direct consequence of the outage. They also must show that they have taken every precaution to prevent the loss themselves, such as by installing uninterruptible power supplies. Given these requirements for torts, the most successful torts have been for food spoilage and mould remediation. (Standler, 2011)

Courts may vary in their definition of "physical damage" when it comes to service interruption coverage. In American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. (2000), the Court ruled that "physical damage" had occurred when a power outage shut down a microcomputer manufacturing plant. In this instance, the term "physical damage" was not restricted to simply physical destruction or harm of computer circuitry, but was stretched to include "loss of access, loss of use and loss of functionality." (Samson, 2000)

In Wakefern Food Corp v. Liberty Mutual (2009) the Court ruled that Liberty Mutual would pay service interruption claims to Wakefern for food spoilage that occurred in their supermarkets during the Northeastern United States 2003 power outage. However, in Fruit and Vegetable Supreme Inc. v. The Hartford Steam Boiler Insp. (2010) and Lyle Enterprizes, Inc. v. Hartford Steam Boiler Inspection and Insurance Co., 399 F.Supp.2d 821 (E.D.Mich. 2005) the court denied the requested service interruption payment for food spoilage during the 2003 outage. (Jackson, Seth)

liability waivers in their contractual agreements, but the courts find against them and they have to contribute to the settlement with the power generation companies. The settlement from the defendants to the power companies are covered as payouts from their insurers and included as defendant company liabilities in our insurance loss estimate. Both sides have significant legal costs.

Companies that lose power

Companies in the affected geographic region of the event footprint (15 states, plus Washington DC) lose power for some period of time, but most are fairly quickly reconnected. The proportion of companies that are affected by outages of different duration is assumed to be the same as the general population of the region, and follow the power restoration curves of Figure 2. Damage and injuries, business disruption, as well as share price devaluation resulting from the outage may all result in insurance payouts.

Perishable contents

The affected region contains an estimated 17,000 large commercial establishments that maintain cold stores and perishable items requiring continuous power operation, including supermarkets, food processing companies, distribution warehouses, laboratories and storage units. We assume that a high proportion of these (80%) have contents insurance. All of these can be expected to have backup generator facilities that will continue to function for some time and maintain power. The average diesel fuelled backup generator carries around 14 days' worth of fuel. When the outage extends across this period, these backup generators lose power, due to the loss of electric-powered gas pumping and shortened supplies from panic buying. In the event of backup generator failure in a long blackout period, perishable contents will ultimately spoil. We estimate that this would affect around 20% of establishments in the S1 scenario (25% in S2 and around 40% in X1). Spoiled contents are claimed under contents insurance with an assumed average claim value, after deductibles, of $50,000 to $500,000, depending on the size of establishment.

The region also contains a further 40,000 small and medium enterprises with smaller capacity cold storage units which have lower insurance penetration (50–70%), very limited backup generator capability, and much smaller average claims ($10,000 to $30,000).

The combined outage losses from these establishments are estimated in the category of companies that lose power – perishable contents.

Contingent business interruption – suppliers extension

It is common for property insurance on large facilities to have a suppliers extension, also known as 'service interruption' cover, or 'utilities extension'. This is a component of 'contingent business interruption' (CBI) coverage for business interruption resulting from lengthy disruption to key utilities such as electrical supply. We have assumed that 'large facilities' are properties with a total insurable value (TIV) of $50m or above. Properties smaller than this do not typically have insurance that includes a suppliers extension.

We estimate that there are around 40,000 large facilities with total insurable value of around $50m or more in the affected region. These include:

- Commercial offices of over 200,000 sq ft
- Major factories, manufacturing, and processing plants
- IT data centres and server farms (Tier 3 & 4)
- Refineries and industrial plants
- Mining and other primary industry operations
- Very large transportation facilities (eg commercial airports/ports/rail terminals)

We believe that in the current market conditions, it is reasonable to assume that 95% of property insurance on large facilities has a suppliers extension.

The suppliers extension covers outage resulting from fire, lightning, explosion, and aircraft impact (FLEXA perils). We assume that the cyber damage resulting in burn-out of the generators and in some cases explosion will be interpreted as fire damage so that losses from the resulting power outage will be covered under suppliers extension. This may be challenged by insurers in practice but our assumption in this estimation is that payouts do occur.

There may be some exclusions that are sustained. Some SE policies have 'territorial limits' and only cover FLEXA events that occur close to the property (eg within 10 miles), and this may be successful in excluding payouts for damage to generators many miles away.

We assume that SE coverages that use CL380 wording, which specifically excludes cyber as a cause of loss, are successful in excluding claims due to the malicious intent of the perpetrators and result in no insurance payouts. However, policies using the standard NMA (2912, 2914 and 2915) wording incur payouts (see the callout box at page 38 for further detail on exclusions).

A variety of deductible periods are applied to SE in the insurance market, typically 28 days or, less commonly, 14 or 7 days. We assume that almost all large facilities in the area have their own backup generator systems but that these can only run for a limited period without refuelling, and that fuelling shortages and delivery difficulties during the outage period will mean that a proportion of large facilities will ultimately suffer outages that exceed their deductible periods. We assume an average daily compensation sum of around $600,000, based on national statistics of average economic output per day from large facilities of this description.

Overall, this is an area of considerable ambiguity and uncertainty, not least due to the interpretation of potential 'silent' cyber coverage but, in our loss estimation with objective assumptions, this coverage and insurance line is likely to be a major driver of insurance loss.

Liability

There are a number of liability insurance coverages that could be triggered by power outages to companies in the affected region. These potentially include, but are not limited to, general liability, errors and omissions, directors and officers, portions of commercial multi-peril coverage, medical malpractice, product liability, and others. Although we expect relatively low levels of bodily injury to result from this scenario, there is potential for deaths and injuries directly related to outage conditions to reach significant levels, as described below. These could trigger significant amounts of liability claims from general liability covers (if deaths occur to third parties from company failures in the blackout), medical malpractice (if hospital or nursing home deaths occur) or from other failures in duty of care.

It is also likely that claims will originate from contractual failures linked to the blackout, such as financial services companies failing to complete electronic transactions or failures by companies to meet their obligations to customers and counterparties.

The most likely area of liability claims is from Directors and Officers (D&O) covers. There is a limited but growing body of case law to support the contention that companies owe a duty of care to their shareholders to maintain risk management procedures to deal with crises. Companies that are adversely affected by the blackout, particularly those that in some way perform worse than their competitors, lose market position and see stock price valuations marked down by analysts, are increasingly likely to see legal actions against the officers of the company by their shareholders.

In our loss estimation, we assume that some proportion of large companies that are badly affected by the blackout suffer class actions from shareholders. We define these as the worst 2% (in S1, 3% in S2 and 5% in X1) of medium to large companies (ie ranging from 100 to 1000 employees). They suffer lengthy outage periods (over five weeks) combined with backup generator failure. The balance sheet loss of quarterly revenue resulting from the power outage is reflected proportionately as stock price devaluation, which shareholders seek to recover with a lawsuit against the officers of the company. The loss estimate assumes some 260 companies see suits of this type in S1, around 500 in S2 and over 1,000 in X1. Shareholders recover around 75% of their claims. Note that we assume that no US corporation of Fortune 1000 status is affected by shareholder action, as these are well diversified geographically and in business activities, and are considered unlikely to be severely impacted in quarterly earnings by a regional blackout.

Companies indirectly affected

Many other companies could potentially be impacted by the sudden disruption of economic activities in the Northeastern United States. They could have business counterparties, trading partners, suppliers, investors, creditors and subsidiaries that are disrupted by the blackout. The indirect consequences on them can cause losses to their insurers.

Contingent Business Interruption (CBI) – critical vendor

Large facilities with property insurance with an extension for CBI may also include 'critical vendor' coverage. This is a separate subordinate contract or 'sublimit' that provides payouts for business interruption that arises from disruption to vital supplies they obtain from other companies. Critical vendor coverage typically covers 'Tier 1' suppliers in a company's supply chain. Accepted practice is to include a schedule of named critical vendors, but this is not always followed. A different set of perils can be specified to the suppliers extension coverage, and may include natural catastrophes but, as with other covers, it may be silent with regard to cyber as the proximate cause of disruption to the critical vendor coverage. We assume that interpretation of peril coverage – ie whether disruption to a critical vendor as a result of power loss resulting from a cyber attack is covered – will be highly contested. Our assumption is that a proportion of these claims are successful.

An example would be 'EndCo.', an electronics assembly company in California that uses parts from 'SupplierCo.', a key circuit board manufacturer in Massachusetts. SupplierCo is a nominated critical vendor on the CBI cover for EndCo. When SupplierCo's operations are disrupted from the cyber blackout and are unable to provide the parts to EndCo, the earnings losses that EndCo suffers are claimed from EndCo's insurers under EndCo's CBI cover for critical vendors.

Note that in the globalised economy, large facilities with CBI insurance for these critical vendors could be located anywhere in the world. Insurance companies could find themselves paying out claims from CBI in markets such as Europe, Southeast Asia and Latin America resulting from the blackout event in Northeastern United States. For this loss estimate, we have only included companies in the United States.

We assume that companies in the blackout area 'fail' (ie cause loss to their EndCos) if their outage is longer than 7 days. The CBI claim by EndCo (number of days of lost business) is the number of days that SupplierCo suffers an outage. EndCos could also be in the affected blackout region. In this case, they could be able to make a suppliers extension claim in addition to a CBI claim from SupplierCo.

There are over 90,000 large facilities (defined – as for suppliers extension – as facilities with total insured value of over $50m) in the United States. We assume 95% of them have CBI cover, and around a third of them (33%) have covers with nominated Tier 1 suppliers. Eighty per cent of their Tier 1 suppliers are in the United States, and reflecting the proportion of the US population that loses power in the Erebos event, 30% of these suppliers are impacted by the blackout. We assume that less than 25% of companies impacted by the blackout fail in their supplier's obligations, and they only result in claims if their supply failure lasts longer than the deductible period in the critical vendor policy sublimit. In all we estimate that around 1,300 companies make a critical vendor claim in S1 variant (2,800 in S2 and 5,500 in X1), with an average daily compensation of around $600,000.

Liability (D&O)

As with companies impacted by blackouts, we expect that companies that suffer as a result of counterparty failures will see claims arising for liability issues, most notably under Directors and Officers cover for failing to have adequate risk management processes in place. This is likely to affect companies that suffer competitively, lose market share and that suffer devaluation of their share price as a result. These are likely to trigger legal actions against the officers of the company by their shareholders and settlements of these are losses for the insurer that provides the company's liability cover. This would be irrespective of whether the company had property insurance with CBI extension that generated a claim from a supplier default.

In the loss estimation we assume that no Fortune 1000 company is affected, but companies of large and medium size (ie ranging from 100 to 1000 employees) are potentially at risk, with around 70% of them having D&O liability cover, and around 25% of them having an important supplier in the impacted Northeastern United States. Of these candidate companies only 2% are disadvantaged (the proportion of suppliers we expect to be more than five weeks in default) and of those only a third perform badly enough to face shareholder action. This results in around 120 companies facing suits for valuation losses of 10–30% in their stock price. We assume that shareholders recover around 75% of their claims through the courts which insurers see as a loss in their liability lines. Both sides have significant legal costs.

Homeowners

Homeowners who suffer property damage to any of their insured assets during the event could be expected to make personal lines insurance claims. This may include damage to cars and houses indirectly resulting from power losses and equipment or alarm malfunctions, potentially including a small number of fires.

Household contents

The most likely cause of large numbers of claims will be from domestic fridge and freezer contents spoilage. Typical HO-3 home insurance policies include standard cover for food spoilage from fridge and freezer defrosting, up to $500. The power outage

would result in domestic fridges and freezers defrosting across the affected area. Any outage of over 24 hours could be expected to result in damage to domestic freezer contents, with longer outages being relatively unimportant in increasing the loss. Around 30% of householders have property insurance, but only 10% have HO-3 contents insurance.[19] We assume that only 50% of potential claimants actually submit a claim, and that the average loss is $400 per claim. We estimate that around 1.2 million households will submit a claim for freezer contents, and that this does not change appreciably in the different scenario variants as the duration of outage is relatively unimportant to the claim frequency.

Specialty

Specialty lines of insurance could see losses resulting from lengthy power outages, including event cancellation or show insurance, livestock and aquaculture insurance and other specialised business activities.

Event cancellation
The main driver of losses in specialty lines is likely to be event cancellation insurance. The number and type of events that are cancelled will depend on the season of the year that the event takes place. In the autumn and winter months there are more professional sport matches and large holiday-related events. In the summer months, there are more open air, theatre and festival meetings.

We have selected to trigger the event in the summer, with the rationale that triggering the event during peak electricity demand will increase the cascading effect of the grid failure and maximise economic impact. However, an event of this type could occur in any season of the year.

The attack in the scenario takes place in July. We assume that events occurring in the affected region during this period will be cancelled if the power is off during the day of the event and up to two days before the planned event will take place. Our modelling does not predict which areas will be reconnected in which order. In general, we assume that the cancellation profile will follow that of the overall population being deprived of power, for example in S1, 50% of the population is without power after 2 days and 25% is without power for 7 days, so 50% of events scheduled for days 3 and 4 are cancelled and 25% of events scheduled for days 8 and 9, and so on.

Across the affected region there are typically several hundreds of events attended by tens of thousands of people scheduled for the summer months of July and August. These include major league baseball games, ATP tennis, PGA golfing tournaments, horse racing meetings, NASCAR motor racing, large stadium rock, pop and classical concerts, music festivals, arts shows, trade shows, political conventions and commercial conferences. There may be a large number of smaller events also insured but we have focused on these 'blockbuster' events.

We assume that 70% of these are insured against cancellation with coverage that includes loss of external power. On average across the affected area and the first four weeks of the event, 21% of events are cancelled. Cancellation costs include ticket sales and lost revenues from TV and sponsorship deals, averaging $2.5m per event. In Scenario S1 we expect claims from around 25 cancelled blockbuster events, in S2, 50 events, and in X1 around 100.

[19] *McKinsey & Company, 2014.*

Additional areas of insured loss not included in estimate

The scenario would almost certainly result in an increase in claims across areas of insurance that we have not included in this estimation. For example:

Injury-related claims
This scenario envisions relatively few people sustaining bodily injury, and so compensation for deaths and injury would likely be minimal. It is possible that people in the generation plants could be hurt by the fire and explosions in the generators, or in fighting the fires. People could be injured in accidents resulting from the blackout. A major public transport accident or plane crash could result in a major insurance payout for injury compensation and liabilities. Heat stress in summer for populations in buildings that lose their air-conditioning could result in hospitalisations and deaths, particularly in the elderly. Hospitals and nursing homes could fail to provide treatments as a result of power loss. There could be riots and social unrest in which people are injured. There could be localised health crises as the effects of the outage wear on.

These situations could give rise to insurance payouts under accident and health covers, workers' compensation, general liability, healthcare insurance, life insurance, and other lines. Overall we do not expect these compensation payouts to be significant drivers of the industry loss and so these are not included in the estimation.

Auto
Auto claims from road traffic accidents would be likely to increase during the initial period of blackout and traffic signal failures, although this could potentially be more than offset by reduced travel as a result of the reduction in economic activity later in the scenario.

Property fire
Accidents and fire ignitions tend to increase during lengthy periods of power outages, partly due to safety and prevention systems going offline. Malfunctioning equipment can trigger fires, and alarm systems that would suppress or reduce the severity of fires may be disabled.

Industrial accidents
There is a significant chance of an industrial accident or a large fire in a major facility. This could significantly increase the overall insurance industry loss.

Environmental liability
The outage could potentially result in industrial accidents that would lead to pollutant release and environmental damage. This could result in significant payouts by insurers under environmental liability coverages held by the companies determined to be responsible.

Social unrest
Past blackouts have prompted rioting and social unrest in urban populations, resulting in looting, criminal damage, arson to buildings, and car fires. This would likely generate property losses for insurers over and above the estimates.

Social unrest would be likely in the event of sustained blackouts.

Insurance vs reinsurance
No attempt has been made to apportion losses between primary insurers and their reinsurers.

Ambiguity in cyber coverage

One of the key purposes of this report is to highlight various issues of exposure that insurers may face from the growing threat of cyber disruption. It identifies some key areas of uncertainty and ambiguity that insurers will need to consider, either in their individual policy coverages, or as a part of the broader portfolio.

Property covers and 'all risks' descriptions are commonly silent on whether cyber-related losses would be paid. Insurers may assume that their exclusion language and conventional interpretation of coverages will protect them from future claims from cyber events, while purchasers of insurance may think they are protected against losses from cyber, where insurers think that these customers have not purchased cover for it.[20]

We suggest that it is clearly in the interests of insurance companies and their corporate customers to clarify the situation, and to be clear about what is and what is not covered. It is important for insurance companies to be properly compensated for the real levels of risks from each of the perils that the policy covers, and for insureds to recognise their risks and the value of obtaining protection through transferring this risk to others.

This mismatch of expectation and reality could be expected to generate disputes in the event of a large scale cyber loss. In this analysis, we have identified a number of areas where there could be significant ambiguity around how coverage will be interpreted and whether claims could reasonably be expected to be successful or denied. These include:

Peril definition
There is ambiguity around the peril definition of cyber and interpretation of whether cyber-related claims would be paid for property damage, suppliers extension or critical vendor contingent business interruption. Our scenario has deliberately invoked fire and explosion to make interpretation of cyber-related payouts more credible as interpretations of the traditional FLEXA perils of fire, lightning, explosion and aircraft impact. If the cyber attack was interpreted as being closer to a natural catastrophe, as it is arguably systemic in nature, then denial of these claims might be upheld.

Event occurrence definition
An additional element of uncertainty is the interpretation of the failures of 50 generators as the occurrence of a single event or multiple events, enabling property generating companies to argue for reinstatements and to optimise deductible payouts. This issue may also arise with respect to the impact of power outages on other claimants.[21]

Territorial limits and specification uncertainties
We have assumed that denial of supplier extension claims are upheld where the policy has territorial limits. We also assume that claims are denied for ambiguity around critical vendor specification and for interpretations around deductibles and event duration.

Exclusion clauses
Many exclusion clauses have been developed for traditional general liability policies to help insurers guard against loss accumulation from cyber events. As described in the breakout box, two of the exclusions (CL 380 and LMA 3030) are designed to prevent claims from cyber events committed with malicious intent or deemed acts of war, while NMA 2912, 2914 and 2915 exclusions are designed to prevent property damage claims from cyber events unless caused by Fire or Explosion. We assume that claims are not paid for coverages that use the CL380 wording.

$5.5bn of uncertainty
We estimate from our modelling of this event, and from the interpretations that we have assumed would be applied, that the insured loss estimation would be increased by at least $5.5bn in the S1 variant if the uncertainties and ambiguities identified above resulted in these denied claims not being upheld.

[20] *HM Government and Marsh, 2015.*

[21] *In All Metals Inc. v. Liberty Mutual Fire Insurance Company, No. 3-09-CV-0846 (N.D. Tex. 2010) , All Metals argued that a power outage that damaged equipment at its metal recycling facility occurred as a series of damage events and that the insurer should pay out $3m in losses. The Court held that the power outage as a whole counted as only one 'occurrence' and Liberty Mutual was only required to pay out $500,000 in losses. (Jackson, Seth V., Zelle Hofmann Voebel & Mason LLP)*

Cyber exclusion clauses (Marsh, 2014).

- Terrorism or Malicious Attacks Exclusions
  - CL 380 – Institute Cyber Attack Exclusion Clause
    - Excludes cover for IT system attacks with the intent to cause harm
  - LMA 3030 – Terrorism Form
    - Excludes cover for attacks attributed to nation-states and deemed an act of war/terrorism
- Property Damage Exclusions
  - NMA 2912 – Information Technology Hazards Clarification clause
    - Also called cyber non-aggregation clause
    - This may be for reinsurers
    - Policy excludes losses arising from computer software, hardware and so on unless property damage is caused by:
      - Fire
      - Lightning
      - Explosion
      - Aircraft or vehicle impact
      - Falling objects
      - Windstorm
      - Hail
      - Tornado
      - Cyclone
      - Hurricane
      - Earthquake
      - Volcano
      - Tsunami
      - Flood freeze
      - Weight of snow
  - NMA 2914 – Electronic Data Endorsement A
    - Policy excludes the loss or damage of electronic data due to any cause (specifically a computer virus)
    - Does cover property damage from loss or damage of electronic data if physical damage is caused by:
      - Fire
      - Explosion
    - The basis for media valuation
    - The cost to repair, replace or restore media
    - Reproduction costs - Including the cost to reproduce the electronic data, limit on the amount
    - If the media cannot be repaired, replaced or restored then the valuation shall be on the cost of the blank media
    - Value of the lost or damaged electronic data is not covered
  - NMA 2915 – Electronic Data Endorsement B
    - Same as NMA 2914, but different valuation
      - Only the cost of the blank media plus costs of copying the electronic data is covered

Government Acts – TRIA and Acts of War

We have framed the scenario to try to avoid the confusion of potential cyber loss with an act of terrorism or an act of war as much as possible. Most insurance contracts have exclusions for a loss caused by an act of war. Terrorism is a specific line of coverage. This report is intended to highlight the potential for large scale systemic losses resulting from cyber threats that may need to be borne by the insurance industry without protection from backstops or political intervention.

Cyber sabotage is notoriously difficult to attribute to an actual perpetrator and there may be events where perpetrators are suspected, but not confirmed. This event as specified represents extensive sabotage of infrastructure and is damaging to the economy, but has no clear perpetrator. Nor is there any evident indication that the event was intended to influence the policy or conduct of the US Government or civilians. We therefore assume that the US Government does not declare the Erebos Event attack as an act of war or terrorism, and that TRIA is not activated.

Activating TRIA[22]
The Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA 2015 or TRIA) was originally enacted in the US in 2002 to help stabilise the insurance market after 9/11.[23] As a result of the major losses experienced from the 9/11 terrorist attacks, many reinsurers left the terrorism market, forcing primary insurers to do the same. The US Government stepped in with TRIA, which required insurers to offer terrorism cover with the government acting as a reinsurer.

The programme triggers when losses from certified acts of terrorism exceed $100m in a programme year.[24] Additionally, in order to access the reinsurance, individual insurers must meet a deductible of 20% of direct earned premiums in the preceding year for covered lines.[25] The US Government will then reimburse insurers for 85%[26] of covered losses from an event certified as terrorism by the Department of Treasury. In order for an event to be certified as an act of terrorism the US Treasury Secretary in consultation with the US Secretary of State and the Attorney General of the United States must determine the event is:

"a violent act or an act that is dangerous to: human life; property; or infrastructure; that resulted in damage within the United States…by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion."[27]

Professional liability lines of coverage were removed from the scope of TRIA when it was first reauthorised in 2005. Most (re)insurance companies treat cyber insurance as a professional liability coverage exempt from TRIPRA. As a result, the cyber insurance market has developed without the expectation of a federal backstop to cap losses.

However, exposure to cyber terrorism extends beyond the coverage traditionally offered by cyber insurance. For example, cyber attacks against Operational Technology can result in physical property losses and bodily injuries by causing explosions or releasing toxic materials. These cyber terrorism events could result in claims against the lines of insurance covered by TRIPRA — such as property and workers' compensation.[28]

Insurance claims by line of business

The matrix at Figure 4 presents our assessment of the impact on claims to all major lines of insurance. Four lines experience 'major' increases in claims, and a total of 32 lines are exposed to some increase in claims.

[22] *The description of TRIPRA 2015 is accurate as of publication. However, significant changes to the programme trigger and insurer co-share will occur over the reauthorisation's lifespan.*

[23] *Further detail on the Terrorism Risk Insurance Program is Available from www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx*

[24] *Beginning in 2016, the trigger increases by $20m each year to reach $200m in 2020.*

[25] *TRIPRA 2015 s.102(7)(A) (15 U.S.C. 6701)*

[26] *Beginning in 2016, the federal reimbursement percentage decreases by 1 percentage point per calendar year until reaching 80%.*

[27] *TRIPRA 2015 s.102(1)(A) (15 U.S.C. 6701)*

[28] *Marsh & McLennan, "Cyber Insurance Falls Outside TRIPRA Concerns", 6 January 2015, [Available Online] https://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/43424/Cyber-Insurance-Falls-Outside-TRIPRA-Concerns.aspx*

Figure 4: Insurance industry loss estimation

We estimate that claims would be triggered under a wide range of classes of insurance, as illustrated below:

CLASS	LINE OF BUSINESS	
Property		
	Personal Lines/Homeowner	0
	Personal Contents	2
	Commercial Combined	5
	Construction & Engineering	1
	Commercial Facultative	4
	Binding Authorities	0
Casualty		
	Workers' Compensation	1
	Directors & Officers	3
	Errors & Omissions	3
	Financial Lines	3
	General Liability	4
	Healthcare Liability	0
	Professional Lines	1
	Professional Liability	2
Auto		
	Personal Lines	-1
	Commercial & Fleet	-2
Marine & Specie		
	Cargo	0
	Marine Hull	0
	Marine Liability	1
	Specie	1
Aerospace		
	Airline	2
	Airport	3
	Aviation Products	1
	General Aviation	1
	Space	0
Energy		
	Downstream	5
	Energy Liability	5
	Onshore Energy & Power	0
	Upstream	0
Specialty		
	Accident & Health	1
	Aquaculture Insurance	0
	Contingency – Film & Event	4
	Equine Insurance	2
	Excess & Surplus	1
	Surety	0

CLASS	LINE OF BUSINESS	
Life & Health		
	Life Insurance	0
	Health Insurance	2
	Income Protection	2
	Death & Disability	0
	Hospital Cover	-3
Pension and Annuities		
	Standard Annuities	0
	Variable Annuities	0
	Enhanced Annuities	0
	Life Settlements	0
War & Political Risk		
	Kidnap & Ransom	0
	Political Risk	2
	Political Violence & Terrorism	1
	Product Recall	3
	Trade Credit	4
Agriculture		
	Multi-peril Crop	0
	Crop Hail	0
	Livestock	0
	Forestry	0
	Agriculture	1
Cyber Cover		
	Standard Data Breaches	1
	Advanced Property	5

KEY TO CHANGE IN INSURANCE CLAIMS	
Major decrease in claims	-5
	-4
	-3
	-2
	-1
No change in claims	0
	1
	2
	3
	4
Major increase in claims	5

Lloyd's conclusions

A cyber attack of this severity is an unlikely occurrence, but we believe that it is representative of the type of extreme events that insurers should assess in order to understand potential exposures. One of the key features of cyber risk brought to life by the scenario is the broad reach of a major event: insurers should consider cyber attack to be a peril that could trigger a wide range of economic losses.

Cyber risk is already an embedded feature of the global risk landscape, and insurance has the potential to greatly enhance cyber risk management and resilience for a wide range of organisations and individuals who are exposed to its impacts. Nevertheless, the likelihood and impact of severe events remain subject to much uncertainty, and the pace of insurance innovation should be linked to the rate at which this uncertainty can be reduced.

This report also reveals the vital contribution of research and analysis in reducing uncertainty concerning cyber risk. Data will be a key factor for enabling further analysis and the development of models to enhance the understanding of cyber risk. The systemic, intangible, constantly evolving nature of cyber threats presents significant challenges for gathering the data required to achieve accurate quantification of the risk for insurance portfolios which could span the global economy. A key mechanism, therefore, by which any insurance or research organisations might be able to achieve the insight needed to capture the full extent of the risk could be enhanced data exchange.

The sharing of cyber risk data is a challenging undertaking involving many complex issues. Examples of sharing arrangements for cyber attack data are already in operation around the world, and these offer the promise that much can be achieved. However, the scale of event described in this report reveals the very wide scope of data that insurers require in order to reduce uncertainty concerning severe events. The sharing of insurance loss data attributable to cyber events among insurers could contribute to this, but this is unlikely to be sufficiently comprehensive in isolation to accurately assess extreme events spanning the full spectrum of threat and every economic sector. Voluntary sharing of cyber attack data, involving a wide range of parties with an interest in developing resilience to cyber attack, offers the most promise for enabling the insurance solutions required to meet this key emerging risk.

Annex A: Cyber attacks against Industrial Control Systems since 1999

Date	Event name	Detailed description	Actors	Motivation	Methodology	Outcome
April 1999 (Milhorn, 2007)	**Gazprom – Russian gas supplier**	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorised Access
July 1999 (National Safety Transport Board, 2002) (Wilshusen, 2007)	**Bellingham**	Over 250,000 gallons of gasoline leaked into nearby creeks and caught on fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb. and April 2000 (Jill Slay, 2008) (Wilshusen, 2007)	**Maroochyshire**	A recently fired employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers and the grounds of a hotel.	Insider attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001 (US House of Representatives, 2005 (SCADA)[29] Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems, 2005	**California**	A hacking incident at California Independent System Operator (CASO) lasted two weeks, but did not cause any damage.	External attack	Unknown and contained	Deliberate	Thwarted
August 2005 (GAO Report, 2007)	**Daimler-Chrysler**	Thirteen Daimler-Chrysler US auto manufacturing plants were taken offline for about an hour by an internet worm. An estimated $14m in downtime costs.		Spyware Installation	Zotob Worm and MS05-039 Plug-n-Play	Infection
Infection	**Brown's Ferry**	Loss of recirculation flow on a US nuclear reactor down for maintenance caused a manual scram. A worm exploited a buffer overflow flaw in the widely used MSSQL server during the scram.		Unknown	Slammer Worm and Buffer Overflow	Non-industrial control systems targets
Oct 2006 (Wilshusen, 2007)	**Harrisburg**	Hackers gained access to a water treatment plant through an infected laptop.	Targeted Threat Agent	Mischief	Compromised Laptop	Server used to run online games
Jan 2008 (Maras, 2012)	**Lodz**	Attacker built a remote control device to control trains and tracks through distributed field devices. Four trains were derailed with zero deaths. A disgruntled employee installed malicious code on a canal control system.	Targeted Threat Actor, Accident or Insider Attack	Mischief	Altered Universal Remote	Mayhem, Criminal Damage
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the E.ON Kingsnorth power station which caused a 500MW turbine to take an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Protest

Contd.

[29] *Supervisory control and data aquisition (SCADA).*

Date	Event name	Detailed description	Actors	Motivation	Methodology	Outcome
Nov 2008 (Kravets, 2009)	**Pacific Energy**	A recently fired employee disarmed safety alarms on three offshore platforms.	Insider Attack	Disgruntled Employee	Disabling alarm systems	Revenge & Sabotage
June 2009 to 2010 (Zetter, 2014)	**Stuxnet**	Malicious code targeted ICS at an Iranian nuclear plant. A recently fired employee disarmed safety alarms on three offshore platforms.	Virus	Unknown Presumed Nation State	Destroying centrifuges and thwarting uranium enrichment	Revenge & Sabotage
2010 to Aug 2014 (Symantec, 2014) (Kaspersky, 2014)	**Dragonfly/Havex/ Energetic Bear campaign**	A campaign against defence, aviation and energy companies	Remote access trojan (RAT)	Espionage	Malware infection and remote access	Malware clean-up
August 2012 (Bronk, 2013)	**Shamoon/ Wiper**	A Saudi Arabian oil company, Saudi Aramco, has over 30,000 workstations knocked out	RAT	Unknown Presumed Hacking group	Wiping 30,000 machines of their data	Unknown
April 2013	**California Power Station**	Snipers fired at a California substation, knocking out 17 transformers.	Physical	Unknown	Destruction of substation oil tanks	Unknown

Annex B: The US electricity grid and cyber risk to critical infrastructure

Structure of the US electricity network

The US power grid consists of three primary components – generation, transmission and distribution – as illustrated at Figure 5:

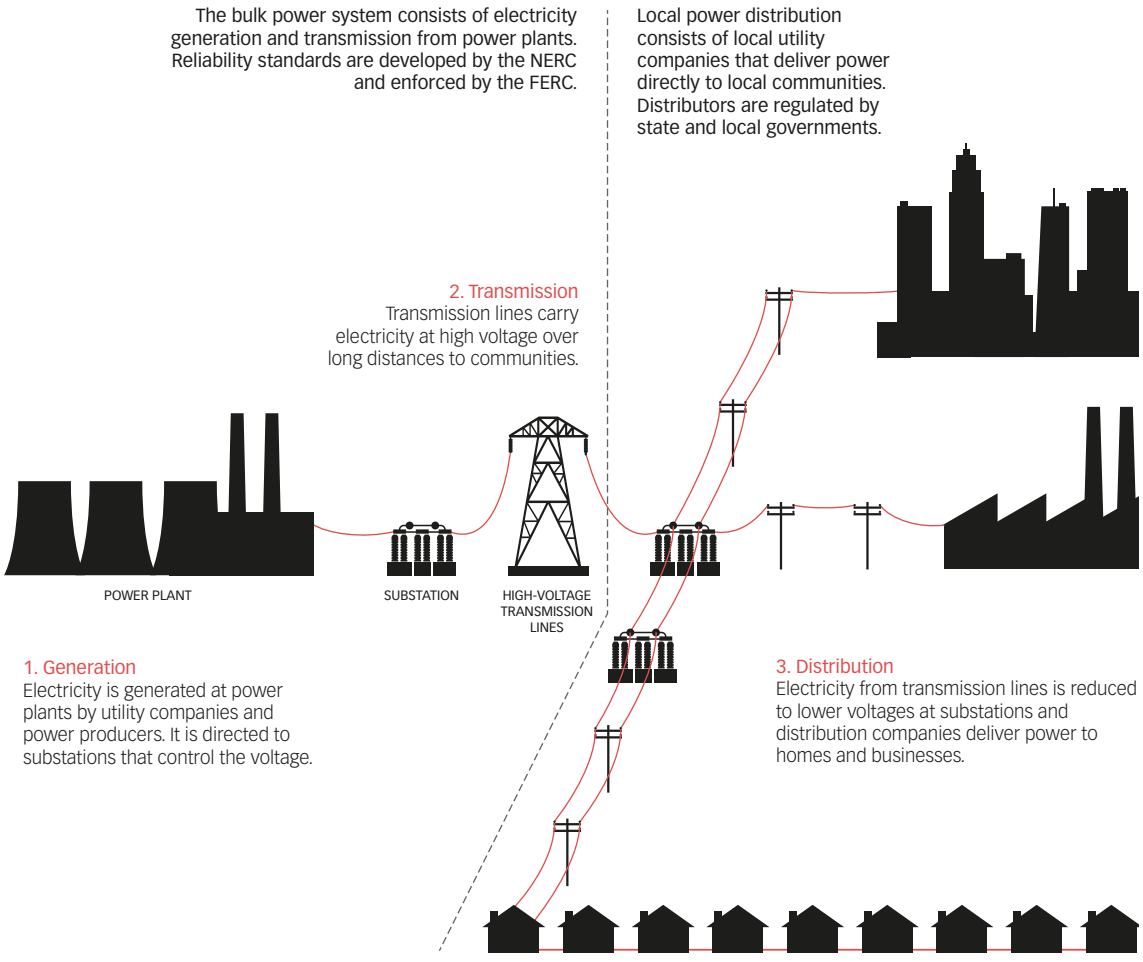
Transmission lines take electricity from power plants and deliver it to cities and towns. Distribution resources and centres reduce the voltage of electricity and deliver to residential consumers, businesses and industrial users.

Electricity is delivered in the USA by three discrete power grid systems or 'interconnects': the Eastern, Western and Texas Interconnections. Transfer of power between these three major interconnects is difficult due to the fact that they operate at different frequency ranges.

The delivery of power within this grid is overseen by the North American Electric Reliability Corporation (NERC), which manages eight reliability regions across the US. Each individual reliability region is responsible for maintaining and improving the reliability of the power supply and abiding by NERC's operating standards. The interconnects and NERC regions are shown at Figure 6 below.

Further detail on the structure of the US electricity network, which was used in the construction of the Erebos Cyber Blackout Scenario, is in the accompanying technical report (Appendix 2, available online).

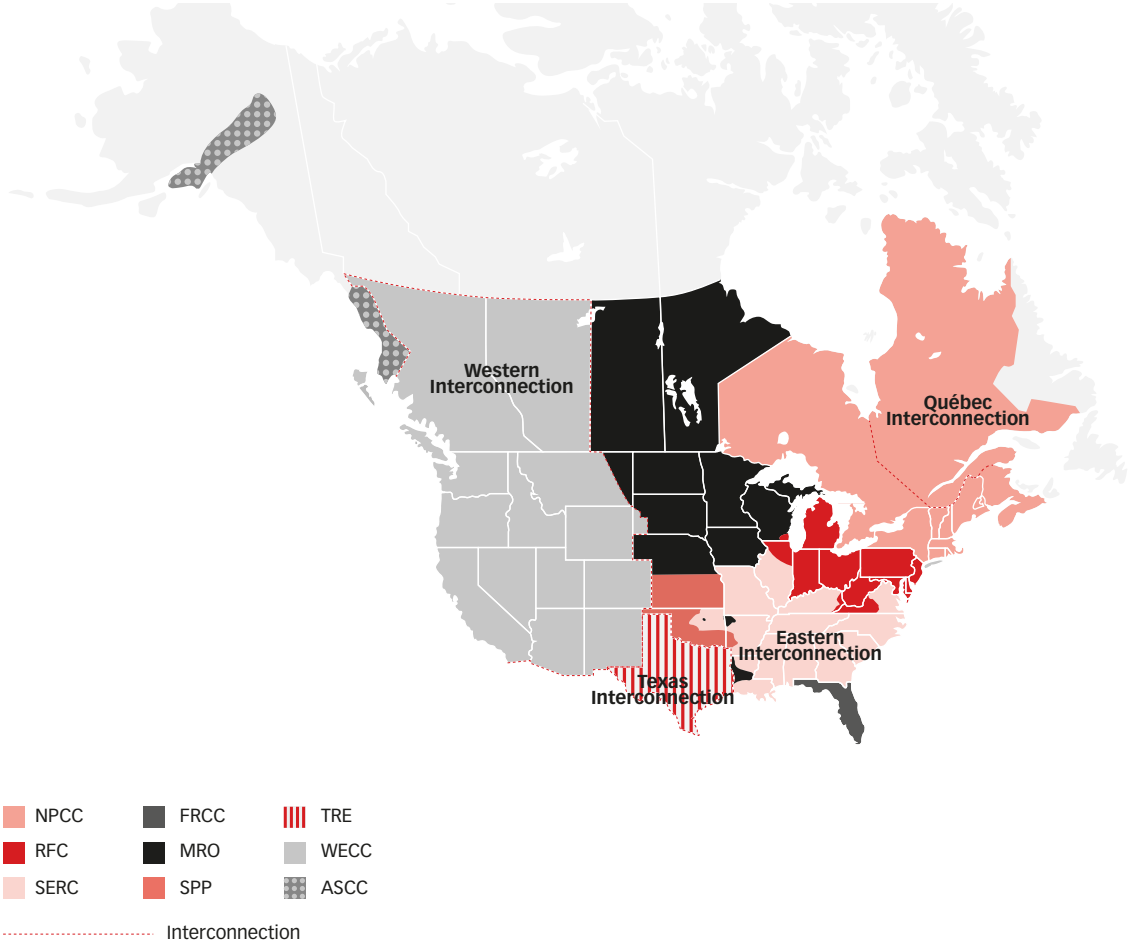
Figure 5: Transmission and distribution grid structure within the US power industry[30]



Note: FERC regulation does not include Texas.

[30] *Information derived from the Heritage Foundation (2014).*

Figure 6: NERC regions within the United States and Canadian electrical grids



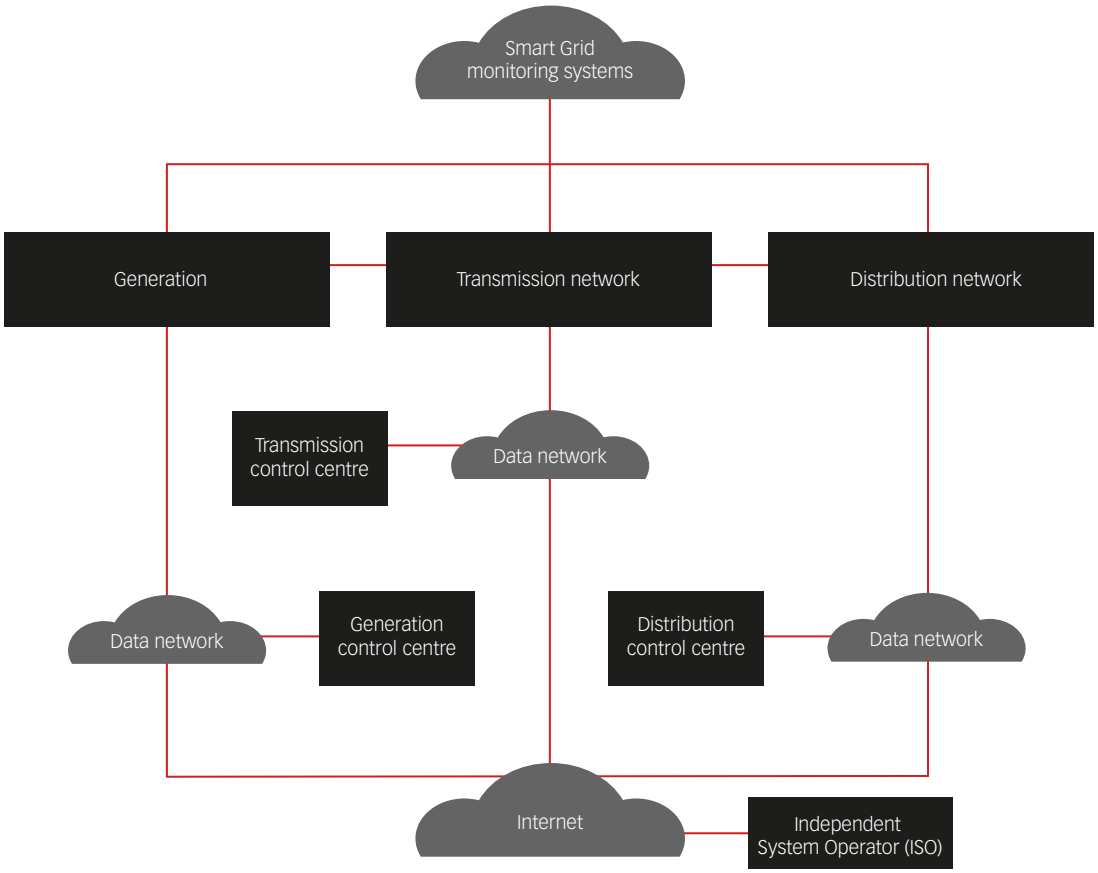
Source: North American Reliability Corporation

Cyber risk and the US electricity grid

Although historically, industrial control systems (ICS) for operation of the electrical grid have been networked locally, many of these systems are now connected to the internet in order to save on costs and improve system reliability. For example, a generation plant is connected to a control room via a corporate IT network which in turn maintains a data connection to the internet. This is a major concern as ICS were not originally developed with network security in mind, potentially giving a hacker a back door into the control rooms and generation plants.

The electrical grid is becoming ever more interconnected through the implementation of the Smart Grid. Smart Grid improvements will enable better monitoring, performance and reliability of the system using thousands of remote controlled measurement devices installed at various points in the grid. Key to the Smart Grid development is the "automation technology that

Figure 7: Current US electricity grid data network, with developing Smart Grid system dimension[31]



lets the utility adjust and control each individual device or millions of devices from a central location."[32] The high connectivity invisaged in the Smart Grid is illustrated at Figure 7.

US critical infrastructure

Critical infrastructure is defined by the US Government as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[33]

Within the critical infrastructure, energy and communications have a key role as they have an 'enabling function', meaning that they are required for the other sectors to operate. The energy sector has three segments: electricity, petroleum and natural gas.

[31] *Office of Electricity Delivery & Energy Reliability, Smart Grid, Technology Development, http://energy.gov/oe/services/technology-development/smart grid*

[32] *Image created by Cambridge Centre for Risk Studies, drawing on information presented in S. Sridhar and M. Govindarsu, Cyber–Physical System Security for the Electric Power Grid, Proceedings of the IEEE. Vol. 100, No.1, January 2012*

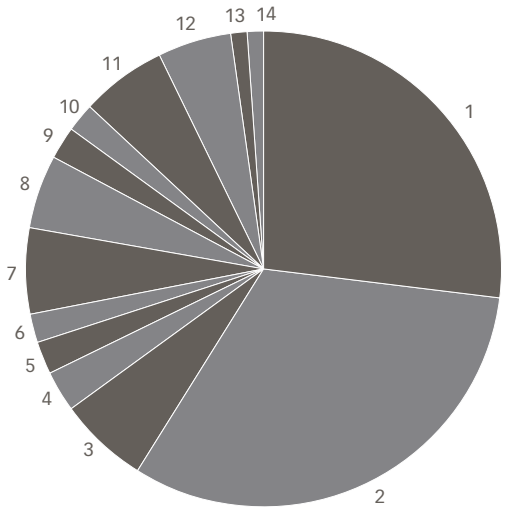
[33] *White House Press Release, Presidential Policy Directive – Critical Infrastructure Security and Resilience, 12 February 2013*

Cyber attacks against ICS and the US power grid

In 2014, the US Industrial Control System Cyber Emergency Response Team (ICS-CERT) reported that 32% of its responses to cyber security threats to critical infrastructure occurred in the energy sector.[34] The full breakdown of ICS cyber incidents by sector is at Figure 8 below:

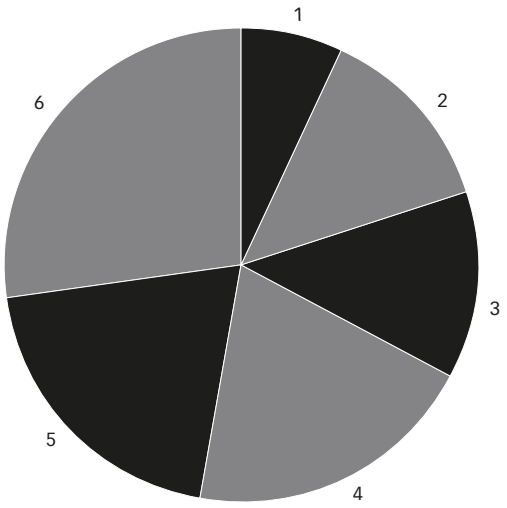
Numerous cyber attacks on critical infrastructure, more specifically on ICS, have occurred around the world, as summarised in the event catalogue at Annex B.[35] ICS is a term that encompasses supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) or programmable logic controllers (PLC). These systems are found in many industrial applications from industrial production to electricity

Figure 8: ICS cyber incidents reported to ICS-CERT, 2014
Source: US Department of Homeland Security, 'ICS-CERT Year in Review'



	Sector	%		Sector	%
1	Critical manufacturing	27	8	Transportation	5
2	Energy	32	9	Nuclear	2
3	Communications	6	10	Information technology	2
4	Commercial facilities	3	11	Healthcare	6
5	Chemical	2	12	Government facilities	5
6	Unknown	2	13	Finance	1
7	Water	6	14	Agriculture	1

Figure 9: Breakdown of suspected cyber attacks on the US grid since 2000[36]



	NERC Region	%
1	TRE	7
2	NPCC	13
3	WECC	13
4	MRO	20
5	SERC	20
6	RFC	27

[34] *US Department of Homeland Security, National Cybersecurity and Communications Integration Center, ICS-CERT Year in Review, Industrial Control Systems Cyber Emergency Response Team, 2014.*

[35] *E. Leverett, Burning Rivers, Sewage in the Lobby and Giant Train Sets, Presentation at National Cyber Security Centre, 23 January, 2013*

generation plants. Electricity generation plants use some form of ICS to control, automate and maintain operation of their equipment and transmission of electricity to the grid.

There have been 15 suspected cyber attacks or events on the US electricity grid since 2000.[37] Forty per cent of these attacks have occurred in the RFC and NPCC regions, as illustrated at Figure 9.

Historical case studies

The Slammer worm attack on Davis-Besse

The Slammer worm created a large amount of network traffic in a nuclear generation facility.
"Davis-Besse had a firewall protecting its corporate network from the wider internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network. This allowed Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network. In response, First Energy set up a firewall between the corporate network and the plant control network.

The Davis-Besse incident highlighted the fact that most nuclear power plants, by retrofitting their SCADA systems for remote monitoring from their corporate network, had unknowingly connected their control networks to the internet. At the time, the Nuclear Regulatory Commission did not permit remote operation of plant functions." (Kesler, 2011)

The Aurora vulnerability

In 2007, Idaho National Laboratory performed several tests to verify the potential for cyber attacks to inflict physical damage on industrial systems. The study showed that a generator could be remotely forced out of phase with the power grid through a compromise in either the protection relay or control signal. Test footage showing the physical impacts of the so-called 'Aurora vulnerability' was later obtained by CNN (Meserve, 2007). The compromise shown in the video resulted in either safety relays isolating the generator (and thus not supplying power), or damage to the bushings, bearings and coupling of the generator. In the case where the safety system works correctly, the generator remains undamaged and intact but no longer supplies electricity to the bulk power system. In the cases where the safety system and protection relays failed or were compromised, the generator was badly damaged and functionally unable to supply power to the bulk power system.

For the purpose of this scenario, we assume that most companies have updated their substation security, but not all, and 10% of generators remain vulnerable. As recently as 2010, discussions were still ongoing about how to improve substation design to mitigate the Aurora vulnerability. One subsequent study found that "standard generator protection is not sufficient to thwart a well-executed Aurora attack." (Zeller, 2011).

[36] *Datasets of electricity disturbance events from Energy.gov and EIA.gov from 2002 to 2014 were used to create the breakdown of suspected cyber attacks. An analysis method presented by Paul Hines, et al, in "Trends in the History of Large Blackouts in the United States" was used to evaluate the dataset. These datasets are compiled from submitted Form OE–417, 'Electric Emergency Incident and Disturbance Report'. Utilities are required by law to submit this form if the outage affects more than 50,000 customers, if outage lasted long than one hour, or if the outage was caused by a physical or suspected cyber attack.*

[37] *US Department of Energy, Office of Electricity Delivery & Energy Reliability, Electric Disturbances Events (OE–417) Annual Summaries*

Annex C: Constructing the scenario – threats and vulnerabilities

A number of potential narratives for the scenario were reviewed and refined with a panel of 30 multi-disciplinary experts, including security specialists, representatives of the power generating companies, government officials and insurance specialists. Elements from real-world events have been blended into the scenario, along with errors in human judgement relating to security architecture and attack detection.[38]

There is a body of literature on cyber-physical attacks against electrical grids. This scenario represents one improbable, but not impossible, narrative.

Difficulties faced by attackers

The scenario describes a cyber attack that disrupts the power supply in the Northeastern United States. We consider who might have sufficient motivation and skills to do this below. However, regardless of access to resources or funding, it is important to highlight how difficult it is to carry out an attack that could achieve this objective.

Regional resilience of grid

The disruption of power delivery in the US cannot be achieved by disabling a single generator. The grid system compensates for losses in generating capacity and manages considerable variation in capacity at any one time, through load balancing and importing power from neighbouring regions via market mechanisms. The regional structure of the US electricity market makes it resilient.

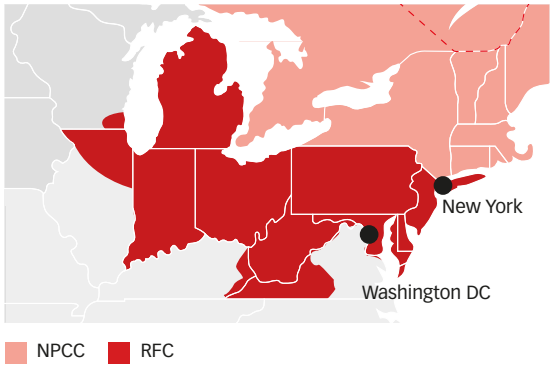
The July 2014 peak-hour electricity demand in the NPCC and RFC regions was 194,000 MW. In order to trigger cascading failures of blackouts across any one region, a sudden reduction of at least 10% in generating capacity is needed at a time of peak demand. This means that attackers seeking to inflict widespread disruption to the grid must take out over 18,000 MW of capacity in these regions.

Focused resources on two regions

Our scenario envisions attackers focusing their efforts on achieving a blackout across two mutually supporting reliability regions, NPCC and RTC, as these serve the high profile economic regions of the east coast including New York, and the political heartland of Washington DC (see map at Figure 10). To extend the blackout to other parts of the United States, the attackers would have to replicate the same effort in the other six regions (Figure 6 above). If the objective of the attack were to disable the entire power supply of the United States it would have to be on a much larger scale and involve greater access to resources, attackers sophistication and coordination than is assumed here. In this scenario, we assume that the intent of the attacker is to demonstrate capability and to achieve a regional blackout rather than to cripple the US economy.

Further detail on the methodology used to select the NPCC and RFC regions as the targets in the Erebos scenario is in the accompanying technical report (Appendix 2, available online).

Figure 10: NPCC and RFC regions



Limitations on damage severity

It is difficult to completely destroy large numbers of generators through software controls. Physical damage sufficient to take the generator offline can be achieved (see callout box on the Aurora vulnerability, page 53), but it is likely that most generators targeted through cyber attack would ultimately be reparable.

Diversity in vulnerabilities

The US power grid is operated by many different companies each with its own systems, technologies, and – importantly – localised vulnerabilities. Certain types of generators and set-up may be vulnerable to a particular type of control mechanism command, but others would not be affected. An attack that is designed to exploit a particular vulnerability can only succeed in systems with that vulnerability.

Vulnerabilities are specific to types of generator hardware, specific manufacturers, the set-up and configuration of the plant control system, the brand of software control system being used, the version of that software, the communication protocols, the security operating environment, and all the different components

[38] *Brenner, (2007)*

of security that need to be overcome to enable the plan to succeed. An attack can be customised to exploit a number of known vulnerabilities in one specific plant but attempting to exploit systemic vulnerabilities across large numbers of plants that operate different combinations of types of generators, different control room configurations and software set-ups is more difficult. It would require the attacker to individually customise their attack to each plant, or take a more generic approach to finding commonality of vulnerabilities, perhaps by trial and error.

Because of this diversity in the systems and components of the plant operations, the attackers are likely to succeed only in a proportion of the places that they attack. The scalability of the attack depends on the standardisation of components and systems in place. In previous cyber scenario research we have identified this concept as 'systemically important technology enterprises' (SITE).[39] In the power generation industry there is significant standardisation, but there is also sufficient variety and diversity in systems to give confidence that the scalability of attacks will be constrained.

Simultaneity of attack
To achieve a power blackout it is important that the attack damages multiple generators simultaneously. An attack that attempted to damage generators one after another over several days would be thwarted by operators identifying a problem after the first two or three incidents and taking generators safely offline to diagnose and remove the problem. This requirement for the attack to occur simultaneously – a 'zero day' attack – is one of the most technically demanding aspects of the sophistication of the attack. It requires software to be either transmitted into control systems at the exact time of the attack, or secretly insinuated into place over time and to remain completely undetectable by routine security checks before being activated by an external signal or a precise internal timer mechanism.

Access to control systems
The most complex part of an attack of this type is likely to be the insertion of the malware into the control systems of the power generating companies at the plants they operate. Generating companies are fully aware of the possibility of cyber intrusion into their systems and have sophisticated security processes, personnel, and a system architecture dedicated to preventing it. Usually, the control systems are separated from the general communications systems of the outside world by a firewall; places where information needs to transfer between the outside world and the control system are heavily screened and policed.

All systems have weaknesses with potential for a determined attacker to find ways through. A sophisticated attacker may be able to devise ways that could exploit vulnerabilities in the defences. In this scenario, we outline four potential vectors that could enable attackers to insert malware into the systems concerned.

Overall logistical burden
Considerable skills and resources would be required to successfully execute a cyber attack to disrupt power supply in the United States. The 'logistical burden' to the attacker of implementing an attack of this type would be high. The attackers would need to research and understand the systems that they are attacking in great detail. They need to identify vulnerabilities they can exploit and they need those vulnerabilities to remain unfixed for long enough for them to design and implement a plan to exploit them. Over time vulnerabilities are addressed and remedied, so there is a limited window of opportunity. A plan is likely to require the identification of multiple vulnerabilities – for example, a way of damaging generators through software controls, as well as a vulnerability to enable malware to be inserted into the control systems. To achieve scale, they need a variety of different approaches to penetrate the diverse systems and types of generators being operated by multiple companies.

They are likely to need a skilled team of operators to create these different code components, to coordinate, monitor and plan, and then to carry out the attack. In our scenario we envision the perpetrators needing to compromise at least 70 different plant control rooms, which is likely to take time, patience and extensive resources.

It will be critical for the attacker team that they are undetected during their preparation and implementation of the attack, which means that they need to evade the active scrutiny of law enforcement agencies, to ensure that any dealings with other parties are secure, and to route all their activities through untraceable channels. They are likely to want to remain undetected after the event to avoid retribution. This requires careful design of the malware which will be forensically examined afterwards, and the channels by which it is delivered.

They may need to obtain some level of assurance that their plan will succeed before they invest in the resources required, and may embark on tests, possibly including practice penetrations of their target facilities. If these tests are detected by the security operators of the facilities they may give themselves away, inviting law

[39] *Cambridge Centre for Risk Studies (2014), Sybil Logic Bomb Cyber Catastrophe: Stress test Scenario*

enforcement response, and they are likely to prompt the rapid fixing of the vulnerabilities that they were planning on using.

Overall the implementation of an operation that successfully disrupts the power supply in the United States would require a significant team of personnel, a high level of skill to create undetectable malware with the functionality required, and many months of careful research, preparation and operational implementation. If this resource requirement were monetised, the attack would require the perpetrators to invest multiple millions of dollars to achieve success.

Who might do such a thing?

In this scenario, we assume that the attack is never officially attributed to a specific perpetrator. One of the characteristics of cyber attacks is the difficulty of attribution. However, the likelihood and realism of a scenario of an attack of this type depends ultimately on whether there are people with the motivation and capability to carry it out. The sophistication of the attack, and the logistical burden required, means that this type of attack is beyond the capability of amateurs, 'script-kiddies', or individual lone actors – it requires an organised team that is well resourced with appropriate infrastructure. There are several categories of cyber threat actor that risk analysts consider in assessing the likelihood of different types of attacks occurring. For each we consider the compatibility of this type of attack with their motivations and capabilities.

Criminal gangs
The large majority of all incidents of cyber crime are for financial gain.[40] Understanding the economics of cyber crime for the perpetrator as well as the victim is an important part of understanding the risk and reducing cyber crime. As with all crime, the threat of being apprehended and punished is a key deterrent, and as cyber law enforcement has improved domestically, cyber crime has increasingly become international, operating through jurisdictions where law enforcement is weak. A grey economy has grown up to support cyber crime that is fuelled by the financial gains it produces. Most activity is relatively minor crime, committed against individuals or small scale operations, but the cyber criminal world has become increasingly organised and sophisticated.

Could a sophisticated criminal gang carry out a cyber attack on the US power grid? It might be possible for a cyber crime gang to develop the high levels of capability required to carry it out, but it is difficult to envision the financial gain that the group would obtain from their attack to make it worth investing the large amount of resources required. Unless there are scenarios whereby the gang extorts money from others, or somehow exploits the blackout for massive criminal gain, it is much more likely that criminal gangs would choose other targets and easier ways to make money from their cyber activities. Criminal gangs are unlikely perpetrators of our chosen scenario.

Hacktivists
Activists campaigning for specific causes have been the instigators of skilled hacking attacks. Causes such as libertarianism, anti-establishment ideology, freedom of information and anti-surveillance, environmentalism, and anti-capitalism have been used to justify cyber attacks that obtain and release information, disrupt business activities, and publicise specific issues. It is conceivable that the ingenuity that hacktivists apply to penetrating corporate networks could be applied to a broader attack on the power grid, perhaps attempting to justify it as some protest against energy consumption or economic inequality. However the exercise would require significantly greater organisational capabilities and resource levels than the community has displayed to date. Hacktivists are unlikely perpetrators of our scenario.

Disgruntled insiders
The knowledge required to carry out damaging attacks is most commonly held by insiders working within the particular industry. There are many examples of insider attacks in companies, institutions and government departments that result from job dissatisfaction, 'whistle-blowing' on wrong-doing, or, in some cases, the desire to draw attention to vulnerabilities. The October 2001 anthrax attacks in the United States are suspected to have been the work of an insider scientist in biodefence labs trying to draw attention to the potential for bioterror attacks.[41] A similar motivation could cause an employee of the power industry to draw attention to vulnerabilities by mounting a demonstration attack. Insiders could also be bribed to sell their domain knowledge to external teams of attackers or participate in an attack for ideological reasons. A single rogue employee would not have the resources to mount the scale of attack that we have specified in this scenario and could not achieve the level of disruption that leads to the losses we describe but could be an important resource to facilitate an attack by other groups.

Terrorist groups
Ever since the Al Qaeda attack of 9/11, 2001, the US has seen external terrorist groups as a key threat to national security. Terrorist groups have proven adept at using information technology for propaganda,

[40] 73.8% of cyber attacks for which a motivation can be ascribed is criminal activity for financial gain, Hackmaggedon.com Feb. 2015 statistics

[41] FBI (2010)

recruitment, and clandestine funding. However, there are very few examples to date of terrorist groups using cyber technologies to mount destructive attacks. In some ways, cyber attack modes may be less attractive to these perpetrators who have historically tended to prefer attacks that can generate high death tolls that spread terror in populations. It is possible that with sufficient additional resources devoted by the terrorist leadership, a terror group could implement an attack on the commercial economy of the United States as a surprise change in tactic. Our scenario however assumes that terrorist groups are not implicated and the event is not declared a terrorist event, which would likely invoke the Terrorism Risk Insurance Act (TRIA).

State-sponsored cyber teams

More than 20 countries are now known to maintain or be developing national cyber teams, with at least six countries having capabilities that analysts consider as 'advanced'.[42] Most of the countries that maintain significant military capability now have cyber units. Several of these countries are potential adversaries of the United States, including North Korea and Iran. Foreign state-sponsored cyber teams from a number of countries are suspected of conducting espionage and information gathering by penetrating systems in the United States; their focus has to date tended to be on military secrets and industrial intellectual property.

Cyber attack could offer a means for hostile states to engage in 'asymmetric' warfare against the United States. The difficulty in assigning responsibility for cyber attacks affords a measure of protection for attackers seeking to avoid provoking retaliation by a stronger opponent, while the dependence of modern societies on digital networks offers the opportunity to create meaningful impacts against the target.

State-sponsored cyber teams have the capability and resources to mount an operation such as the scenario envisioned here. However even adversaries have generally avoided any direct action that would provoke an American response. Our scenario avoids having an attack that is recognised as a formal act of war. It is possible to envision situations of either miscalculation by a potential sponsor state or a state using a proxy organisation to carry out a demonstration attack, perhaps as a warning or deterrent to United States foreign policy. It would likely involve concealment or complex routes of attribution to avoid or complicate American response. There are strong deterrents for nation states in executing an attack on the US but hostile state-sponsored cyber teams are one of the few potential candidates with the resources to perpetrate a scenario of this type.

Scale and severity

The Northeastern United States was selected as the area of focus because of its major city targets and the diversity of its population, commercial interest, contribution to US overall GDP, and previous blackouts history. The scenario affects the two reliability regions of NPCC and RTC.

The analysis of the US power grid demonstrates that for cascading failure to occur in these two regions, the scenario needs to result in the sudden removal of around 18,000 MW of capacity during periods of peak loads.

[42] *Lewis (2102).*

The three scenario variants were designed to roughly correspond to the severity of power capacity losses that might be expected from accidental causes or weather events with an annual probability of 1 in 50 (S1), 1 in 100 (S2) and 1 in 200 (X1).

In the target reliability regions of NPCC and RTC, there are 676 generators with capacities above 100 MW and up to 1,400 MW, operating under the supervision of 261 power plants. Nuclear power plants were excluded from the scenario. Analysis of capacity of generators shows that it would be possible to remove 18,000 MW by taking around 50 generators offline. The extreme scenario variant, X1, has 100 generators taken offline. This increases the duration of the outage, but not the geographical extent of the impact, and increases the severity of the economic and insurance loss.

In the standard scenario, 50 generators are taken offline by a malicious malware attack. Our analysis does not specify which specific generators they are. There are many geographical permutations of damage which would achieve the same loss of generator capacity. A number of simulations were run to assess numbers of generators that might be affected, accounting for variables in the malware's range of access and unique system vulnerabilities.

Designing an extreme cyber event

Insurance companies are familiar with applying scenarios for natural catastrophes and other extreme events, using a statistical claims history or a catastrophe model based on scientific observations. For cyber events, there is little to no claims history or probabilistic catastrophe modelling to identify the scenario of interest.

Developing a severe cyber attack scenario without a probabilistic description of expected severities from future events is a statistically challenging task. Computers have been with us since the 1940s but have only been ubiquitous since the 1980s. There is no database containing a century's worth of detailed cyber attack history to draw upon in designing this study. Due to various schemes for reputation management and data sharing laws, the majority of Operational Technology attacks over the last 20 years have not been made public, making even a catalogue of recent reference events difficult to assemble. In order to properly gauge a severe event of low probability an extreme event analysis was performed on historical US power outage data for the period 2002–2014. Further details are described in the accompanying technical report.

This disaster scenario also has to strike a crucial balance between depicting a credible potential cyber attack and not outlining how exactly to carry one out successfully. This scenario should be read as improbable but not impossible and aims to promote debate and discussion in order to prepare the insurance market to handle the risk of an extreme cyber attack on the power grid and its wider impact.

Bibliography

1. Anderson, R., 1994. Liability and Computer Security: Nine Principles. In: Gollman, D., ed. *Computer Security – ESORICS 94*. Berlin: Springer-Verlag. pp.231-245. Available from: www.cl.cam.ac.uk/~rja14/Papers/liability.pdf

2. Bliem, M., 2009. *Economic Valuation of Electrical Service Reliability in Austria - A Choice Experiment Approach*. Available from: www.researchgate.net/profile/Markus_Bliem/publication/261228939_Economic_Valuation_of_Electrical_Service_Reliability_in_Austria_-_A_Choice_Experiment_Approach/links/02e7e533a87b3a07c2000000.pdf

3. Brenner, S., 2007. At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 97(2). Available from: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc

4. Bronk, C. & Tikk-Ringas, E., 2013. *Hack or attack? Shamoon and the Evolution of Cyber Conflict*. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2270860

5. Bruch, M., 2013. *NatCat and Power Blackout Risks*. Allianz Global Corporate & Specialty. Available from: www.agcs.allianz.com/assets/Global%20offices%20assets/Germany/NatCat%20and%20Power%20blackout%20risks_AGCS%20ED%202013_final.pdf

6. Cambridge Centre for Risk Studies, 2014. *Sybil Logic Bomb Cyber Catastrophe Scenario: Stress test Scenario*; Cambridge Centre for Risk Studies Cambridge Risk Framework. Available from: http://cambridgeriskframework.com/getdocument/9

7. Carlsson, F., Martinsson, P. and Akay, A., 2011. The effect of power outages and cheap talk on willingness to pay to reduce outages. *Energy Economics*, 33(5), p.790–798. Available from: www.sciencedirect.com/science/article/pii/S0140988311000247

8. CRO Forum, 2014. *Cyber resilience: The cyber risk challenge and the role of insurance*. Available from: www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/

9. Daly, E.M., 2010. FERC Fines Fla. Power Grid Agency Over Blackout. Law360. Available from: www.law360.com/articles/153950/ferc-fines-fla-power-grid-agency-over-blackout

10. DeJesus, J. and Halpern, J., 2013. FERC Imposes a $975,000 Civil Penalty Against Entergy for 27 Violations of Reliability Standards. *Energy & Environmental Law Adviser*. Available from: www.energyenvironmentallawadviser.com/2013/04/ferc-imposes-a-975000-civil-penalty-against-entergy-for-27-violations-of-reliability-standard/

11. Electric Power Supply Association, 2007. *Electricity Primer – The Basics of Power and Competitive Markets*. Available from: https://www.epsa.org/industry/primer/

12. Eto, J., Koomey, J., Lehmen, B., Martin, N., Mills, E., Webber, C. and Worrell, E., 2001. *Scoping Study on Trends in the Economic Value of Electricity Reliabilty to the US Economy*. EPRI. Technical report. Available from: http://emp.lbl.gov/sites/all/files/REPORT%20lbnl%20-%2047911.pdf

13. Federal Bureau of Investigation, 2010. *Amerithrax Investigative Summary, Released Pursuant to the Freedom of Information Act*. Available from: www.justice.gov/archive/amerithrax/docs/amx-investigative-summary.pdf

14. Government Accountability Office, 2007. Report to Congressional Requestors: *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*. GAO-07-1036. Washington DC: Government Accountability Office. Available from: www.gao.gov/new.items/d071036.pdf

15. Government Accountability Office, 2007. *Critical Infrastructure Protection: Testimony GAO-08-119T*. Washington DC: Government Accountability Office. Available from: www.gao.gov/highlights/d08119thigh.pdf

16. The Heritage Foundation, 2014. The Grid: How Electricity is Distributed and Regulated. Available from: www.heritage.org/multimedia/infographic/2014/10/the-grid-how-electricity-is-distributed-and-regulated?ac=1

17. Hines, P., Apt, J., and Talukdar, S., 2008. *Trends in the History of Large Blackouts in the United States*. Available from: www.uvm.edu/~phines/publications/2008/Hines_2008_blackouts.pdf

18. HM Government UK and Marsh Ltd., 2015. *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*. Available from: https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

19. Hynes, J., 2009. *How to Compare Power Generation Choices*. Available from: www.renewableenergyworld.com/articles/print/rewna/volume-1/issue-1/solar-energy/how-to-compare-power-generation-choices.html

20. Jacobs, M., 2013. Thirteen of the Largest Power Outages in History – and What They Tell Us About the 2003 Northeast Blackout. *The Equation*. Available from: http://blog.ucsusa.org/2003-northeast-blackout-and-13-of-the-largest-power-outages-in-history-199

21. Jackson, S., 2012. Ensuring Service Interruption Coverage. *Insurance Law360*. Available from: www.zelle.com/news-publications-191.html

22. Kaspersky, 2015. *Crouching Yeti | Energetic Bear Malware Threat*. Available from: http://usa.kaspersky.com/internet-security-center/threats/crouching-yeti-energetic-bear-malware-threat

23. Kesler, B., 2011. The Vulnerability of Nuclear Facilities to Cyber Attack. *Strategic Insights*, Spring 2011. Available from: https://calhoun.nps.edu/handle/10945/25465

24. Klinger, C., Landeg, O. and Murray, V., 2014. Power Outages, Extreme Events and Health: A Systematic Revoew of the Literature from 2011-2012. *PLoS Currents*. Available from: www.ncbi.nlm.nih.gov/pmc/articles/PMC3879211/

25. Knapton, S., 2008. Power station break-in sparks security review. *The Daily Telegraph*. Available from: www.telegraph.co.uk/news/uknews/3705073/Power-station-break-in-sparks-security-review.html

26. Kravets, D., 2009. USA v Mario Azar. *Wired*. Available from: www.wired.com/images_blogs/threatlevel/files/azar.pdf

27. LaCommare, K.H. and Eto, J.H., 2004. Understanding the cost of power interruptions to US electricity consumers. *Lawrence Berkeley National Laboratory*. Available from: https://escholarship.org/uc/item/1fv4c2fv.pdf

28. Leverett, E., 2013. *Burning Rivers, Sewage in the Lobby and Giant Train Sets*. Presentation at National Cyber Security Centre, January 23, 2013. Available from: https://www.ncsc.nl/english/conference/conference-2013/speakers/eireann-leverett.html

29. Lewis, J., 2012. *Cybersecurity, Threats to Communications Networks, and Private-sector Responses: Testimony to House Committee on Energy and Commerce, Subcommittee on Communications and Technology, February 8, 2012; submission by Center for Strategic and International Studies*. Available from: http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Lewis-CAT-Cybersecurity-Threats-2-8-2012.pdf

30. Maras, M-H., 2012. *Computer Forensics: Cybercriminals, Laws, and Evidence*. Burlington: Jones & Bartlett Learning.

31. Marsh, 2014. *Cyber Cap Insurance – Cyber Risk: Filling the Coverage Gap*. Available from: http://uk.marsh.com/Portals/18/Documents/Cyber%20Gap%20Insurance%20Brochure_Final.pdf

32. Marsh, 2015. *Cyber Insurance Falls Outside TRIPRA Concerns*. Available from: https://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/43424/Cyber-Insurance-Falls-Outside-TRIPRA-Concerns.aspx

33. McKinsey & Company, 2014. Global insurance industry insights: an in-depth perspective. Available from: www.mckinsey.com/client_service/financial_services/latest_thinking/insurance

34. Merchant, A., and Thompson, M., 2010. The Electric Power Transmission and Distribution Industry. InContext, Vol. 11, No. 4. Available from: www.incontext.indiana.edu/2010/july-aug/article3.asp

35. Meserve, J., 2007. Staged cyber attack reveals vulnerability in power grid. CNN, 26 September 2007. Available from: http://edition.cnn.com/2007/US/09/26/power.at.risk/

36. Milhorn, H., 2007. *Cybercrime: How to Avoid Becoming a Victim*. Boca Raton: Universal Publishers

37. National Association of Insurance Commissioners, 2015. *Terrorism Risk Insurance Act (TRIA)*. Available from: www.naic.org/cipr_topics/topic_tria.htm

38. National Transportation Safety Board, 2002. *Pipeline Rupture and Release of Gasoline, Olympic Pipeline Company. NTSB/PAR-02/02 PB2002-916502*. Washington DC: National Safety Transport Board. Available from: www.ntsb.gov/investigations/AccidentReports/Pages/PAR0202.aspx

39. Nazarian, D., 2012. *Introduction to US Electricity Markets*. Presented at NARUC/CAMPUT Bilateral Roundtable, 12 July 2012. Available from: www.camput.org/wp-content/uploads/2013/09/2012-07-21_-Nazarian_US_Electricity_Markets.pdf

40. New York Independent System Operator, 2014. *Power Trends 2014: Evolution of the Grid*. Available from: www.nyiso.com/public/webdocs/media_room/publications_presentations/Power_Trends/Power_Trends/ptrends_2014_final_jun2014_final.pdf

41. North American Electric Reliability Corporation, 2013. *Regional Entities: NERC Interconnections*. Available from: www.nerc.com/AboutNERC/keyplayers/Pages/Regional-Entities.aspx/

42. Office of Electricity Delivery & Energy Reliability, 2014. *Electric Emergency Incident and Disturbance Report*, OE-417. Available from: https://www.oe.netl.doe.gov/docs/OE417_Instructions_03312018.pdf

43. Office of Electricity Delivery & Energy Reliability, 2015. *Smart Grid*. Available from: http://energy.gov/oe/services/technology-development/smart-grid

44. Office of Electricity Delivery & Energy Reliability, 2015. *Submissions of all Electric Emergency Incident and Disturbance Reports (OE-417)*. Available from: www.oe.netl.doe.gov/oe417.aspx

45. Peace, R., and Tweed, C., 2014. FERC Approves $3.25 Million Civil Penalty in Southwest Blackout Case. *Energy Legal Blog*. Available from: www.energylegalblog.com/archives/2014/07/08/5685

46. Ponemon Institute, 2015. *2014: a Year of Mega Breaches*. Available from: www.ponemon.org/library/2014-a-year-of-mega-breaches

47. Reichl, J., 2013. Power Outage Cost Evaluation: Reasoning, Methods and an Application. *Journal of Scientific Research and Reports*, 2(1), p.249–276. Available from: www.sciencedomain.org/abstract/1229

48. Reichl, J., Schmidthaler, M. and Schneider, F., 2013. The value of supply security: The costs of power outages to Austrian households, firms and the public sector. *Energy Economics*, 36, p.256–261. Available from: www.researchgate.net/publication/256967848_The_value_of_supply_security_The_costs_of_power_outages_to_Austrian_households_firms_and_the_public_sector

49. Rid, T.,2013. *Cyber war will not take place*. London: Hurst & Company

50. Royal Academy of Engineering, 2014. *Counting the cost: the economic and social costs of electricity shortfalls in the UK*. Available from: www.raeng.org.uk/publications/reports/counting-the-cost

51. Samson, M., 2000. *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299. Available from: www.internetlibrary.com/cases/lib_case155.cfm

52. Slay, J. and Miller, M., 2008. Lessons Learned from the Maroochy Water Breach. In: Goetz, E & Shenoi, S, eds. *Critical Infrastructure Protection* Springer: IFIP. pp. 73-82.

53. Sridhar, S. and Govindarsu, M. 2012. Cyber-Physical System Security for the Electric Power Grid, *Proceedings of the IEEE*. Vol. 100, No.1, January 2012.

54. Stamp, J. D., Dillinger, J., Young, W. and DePoy, J., 2003. *Common Vulnerabilities in Critical Infrastructure Control Systems*. Albuquerque: Sandia National Laboratories. Available from: www. energy.sandia.gov/wp-content/gallery/uploads/031172C.pdf

55. Standler, R., 2011. *Liability of Electric Utility in the USA for Outage or Blackout*. Available from: www.rbs2.com/outage.pdf

56. Symantec, 2014. *Dragonfly: Cyberespionage Attacks Against Energy Suppliers*. Available from: www.symantec.com/en/uk/outbreak/?id=dragonfly

57. Symantec, 2015. *2015 Internet Security Threat Report*. Available from: http://know.symantec.com/LP=1123

58. Tripwire, 2013. *NERC CIP: It Gets Worse Before it Gets Better*. Available from: www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip-it-gets-worse-before-it-gets-better/

59. US Department of Energy, Office of Electricity Delivery & Energy Reliability, 2015. *Electric Disturbances Events (OE-417) Annual Summaries*. Available from: https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

60. US Departments of Energy and Homeland Security, 2010. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Available from: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_2010.pdf

61. US Department of Homeland Security, 2014. *Cyber Insurance Roundtable Readout Report, Health Care and Cyber Risk Management: Cost/Benefit Approaches*. Available from: www.dhs.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf

62. US Department of Homeland Security, National Cybersecurity and Communications Integration Center, 2014. *ICS-CERT Year in Review, Industrial Control Systems Cyber Emergency Response Team*. Available from: https://ics-cert.us-cert.gov/Year-Review-2014

63. US Energy Information Administration, 2015. Electricity Data Browser. Available from: www.eia.gov/electricity/data.cfm

64. US Energy Information Administration, 2015. Electric Power Monthly Data, Major Disturbances and Unusual Occurrences, Year-To-Date 2015. Available from: www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_b_1

65. US Energy Information Administration, 2015. Wholesale Electricity and Natural Gas Market Data, February 2015. Available from: www.eia.gov/electricity/wholesale/ [Accessed: February 2015]

66. US House of Representatives, Committee on Homeland Security, 2005. *SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems*. Available from: www.fas.org/irp/congress/2005_hr/scada.pdf

67. US Iter Project, 2008. *Examples of Major Bulk Electric System Power Outages*. Available from: http://fire.pppl.gov/blackout_history_table.pdf

68. USA Today, 2015. *Outages hit D.C., including White House, Capitol*. Available from: www.usatoday.com/story/news/nation/2015/04/07/power-outages-dc/25411847

69. The White House, Office of the Press Secretary, 2013. *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. Presidential Policy Directive/PPD-21. Available from: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

70. World Economic Forum 2015. *The Global Risks Report 2015*. Available from: www.weforum.org/reports/global-risks-report-2015

71. Zeller, M., 2011. *Common Questions and Answers Addressing the Aurora Vulnerability*. Available from: https://www.selinc.com/workarea/downloadasset.aspx?id=9487


FIDENTIA