Jeanne Sheehan

4 Beyond lip-service: Content clouds, 10-K filings, cyber risk and the electric grid

4.1 Introduction

In the spring of 2021, two major companies operating in the United States were hit by back-to-back ransomware attacks. The first attack shuttered Colonial Pipeline; one of the nations' largest oil pipelines which runs 5,500 miles from the Texas Gulf to New England and serves major portions of the eastern coast. The shutdown sparked widespread fears of a gas shortage and led to both an increase in oil prices and panic buying up and down the Atlantic seaboard (Uren, 2021).

Shortly after, JBS Foods – one of the world's largest meat suppliers – fell victim to cyber criminals who demanded a similarly exorbitant payout. The attack forced the company to temporarily halt production at its U.S. plants and led to both price increases and panic buying.

While the Colonial and JBS attacks received a good deal of media attention, these companies were not alone. Around the same time, the Metropolitan Transportation Authority (MTA), the nation's largest transit authority which serves the New York City metro area, suffered its third and most significant attack (Goldbaum et al., 2021). And earlier in the year, it was discovered that there was an unsuccessful attempt by cyber criminals to poison the water supply in Oldsmar, Florida. The Oldsmar attack came on the heels of another major cyber-attack – the SolarWinds hack – that was uncovered in December of the previous year. In that instance, hackers were able to intrude on and leverage software made by SolarWinds – which serves 18,000 customers – to infiltrate and compromise at least nine U.S. federal agencies and more than one hundred private sector companies, including some operating in the energy and electric sector (The SolarWinds, 2021).

What is notable about all these attacks is that each targeted key sectors of America's infrastructure – oil, food, transportation, water, energy, and electricity. In striking critical industries, these hackers showed not only how vulnerable the nations' infrastructure is but how disruptive and potentially deadly a successful attack might be. While the Colonial and JBS attacks were short-lived and only briefly disrupted some American's – more inconvenience than crisis; nevertheless, for many they portended much more deadly and consequential attacks to the nation's infrastructure. As Rick Tracy, Chief Security Officer and Product Manager at Telos Corporation said, "imagine a similar attack on the power grid in the dead of summer. How many heat-related deaths might occur in the hottest parts of the country (quoted in Walton, 2021)?"

It is this type of fear that, in the wake of these attacks, ultimately seemed to catch the attention of not just of the public and media, but those at the highest levels

Open Access. © 2023 the author(s), published by De Gruyter. BY-NC-ND This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
https://doi.org/10.1515/9783110731217-004

of government. Shortly after the pipeline attack, President Biden became the first president in American history to speak publicly about the threat of ransomware. At the same time, he announced the creation of a cyber-security task force within the Department of Justice (DOJ) to investigate the growing number of attacks, specifically focusing on the risks to America's critical infrastructure and national security.

The seriousness that these threats were being taken was reinforced by FBI Director Christopher Wray who compared the spate of cyber-attacks against the U.S. to the 9/11 terror attacks. He stated, "there are a lot of parallels, there's a lot of importance, and a lot of focus by us on disruption and prevention (Viswanatha et al, 2021)." He went on to confirm that the number of reported incidents to his agency show that ransomware attacks in the U.S. had tripled over the last year (Baker, 2021).[1]

There is no question that these incidents cast an unprecedented level of governmental, public, and media attention on cyber-attacks. To this extent they were, in the words of Tobias Whitney, vice president of Fortress Information Security, 'eye-opening.' A "wake-up call to the rest of the critical infrastructure industries," Whitney said, "to really make sure we are not just giving lip service to these issues (quoted in Miller, 2021)."

But are critical infrastructure industries taking these threats as seriously as Whitney and other experts suggest they should? And if so, how seriously? How does the threat of cyber-attack rank when compared with other critical risks these organizations are facing? This article sets out to provide answers to these questions by focusing on one of the most vulnerable infrastructure sectors – energy, and in particular, the electricity segment. First, however, it is important to look at where cyber threats fit within our traditional conception of 'political risk.'

4.2 Re-conceptualizing political risk to meet 21st century threats

In "Note on Political Risk Analysis" Heidi Deringer and Jennifer Wang (1997, 1) define political risk as a "broad concept" that refers "to the possibility that political decisions or events in a particular country will cause foreign investors there either to lose money or fail to capture their expected returns." They (1997, 1) go on to argue that it "arises from the vagaries of governmental action: from policy changes, leadership changes, nationalization of private property, expropriation of foreign holdings, civil strife, currency inconvertibility, or even war."

1 It is remains difficult to determine exactly how many cyber-attacks have taken place in the United States because there is no centralized agency that tracks them, consequently, many continue to go unreported (Shue, 2019).

Writing more than two decades later, Condoleezza Rice and Amy Zegart (2018a; 2018b) take issue with this type of definition, which they describe as outdated because of its limited conception of risk generators. In the 21st Century, they argue, no longer is the threat merely from governmental actors, but political actors more broadly defined. "Political risk," they (2018a, 3) write, "is essentially the probability that a political action will significantly affect business –whether positively or negatively." They go on to note that they (2018a, 3) chose the phrase 'political action,' as opposed to 'government action,' in an effort to "highlight the growing role of risk generators outside the usual places like capitals, army barracks, and party headquarters."

Rice et al's contributions in this area should be applauded. Not only do they recognize the need to expand risk generators beyond the traditional scope of governmental actors, but they also highlight something critical to this series, that the impact is not only potentially negative, but positive as well (Engemann et. al., 2021).

Despite this, as we examine it from the perspective of 21st century threats such as ransomware and cyber-attacks, their reconceptualization falls short in two areas. The first, is its tendency to focus on the motives of the actor. Rice et al. (2018a, 3) describes their re-definition as "radical" because the generator is no longer merely a government or governmental entity, but a political action coming from any actor who is politically motivated (i.e., documentarians, terrorists, etc.). Unfortunately, by linking the new definition to motive, they run into a conundrum long noted by post-structuralists and find themselves with a definition that is not as modern or all-encompassing as they claim.

In another realm, John Searle (1993) famously argued that 'truth' is independent of motive. In a similar vein, a more 'radical' conception of risk fit for the 21st Century should resist the tendency to find political risk only in cases where the motive of the actor is known. In short, political risk should be independent of the motives of the generator if only because motive is perennially difficult to know and often changing.

Consider, for instance, ransomware attacks of the type we witnessed with Colonial and JBS. Under Rice et al.'s (2018a) definition of risk, the motive of the hackers (i.e., the generators) would have to be 'political' for these attacks to qualify as creating 'political risk' for these organizations. Yet in the case of Colonial, that type of designation is difficult to assess. The U.S. government has attributed the attacks to a group called DarkSide believed to be operating in Eastern Europe, but not, as far as officials have acknowledged to date, connected with the Russian government or any governmental or political body. More importantly, shortly after the attack, DarkSide addressed the shutdown and explicitly noted that they were not politically motivated. As they wrote on their web site: "we are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for our motives. Our goal is to make money (quoted in Javers, 2021)." The veracity of this statement aside, it underscores how difficult it is to attribute motive, as well as how easy it would be to imagine information and evidence coming forward in the future which refutes their claims.

It is for this reason that as we think about ransomware attacks in particular, it makes sense to avoid tying the existence of political risk to the motives of the generator. In the DarkSide example, there are cases where an actor may be motivated by something other than politics or, alternatively, their motives may be unknown, unknowable, unclear, or mutable. Nevertheless, their actions can and do present political risk to an organization. The issues in these instances are not necessarily the motives of the actors, but rather the state of the political environment in which they are operating – in these cases, an atmosphere that allows them to engage in behavior which creates political risk for an organization.

Consider the example of a company that is interested in setting up a factory in a country where the risk of kidnapping is high. In this scenario, you can postulate the 'kidnappers' are not motivated by politics but rather by economic interest. Most risk analysts would agree that any company looking to establish business interests in that geographical area would accept a certain amount of political risk. In this case, the hypothetical political risk stems not from the motives of the kidnappers, but rather the state of governance (or lack thereof) on the ground in the country in which they are operating.

The same is true in the case of a ransomware attack. If we accept their claim as fact just for purposes of this hypothetical scenario, we can adopt the assumption that a group of hackers like DarkSide may not be politically motivated. That does not mean, however, that they did not pose a grave political risk to Colonial. Just as in the case of our hypothetical kidnappers, their motives were not a factor. Instead, it the fact that the company was operating in an environment that that did not contain the proper governmental safeguards to protect them from cyber-attack. In this case the lack of governance can come from a variety of arenas including the countries or areas in which the hackers are operating and the countries or areas in which the company is operating. This may also include the failure of cyber security experts both internal to the company and/or outsourced by them, to secure the space.

The second area where both Deringer et al.'s (1997) and Rice et al.'s (2018a; 2018b) work on conceptualization falls short, particularly in the context of this volume, is that they focus almost exclusively on risks to corporations and businesses versus other types of organizations such as public sector entities, quasi-public entities, and those operating in the non-profit arena. As we focus on critical infrastructure in the U.S., we find a host of different types of organizations impacted by cyber threats. Consider that the four cyber-attacks in early 2021 were against Colonial (a privately owned company), JBS (a publicly traded company), the MTA (a public transport agency), as well as an attempted hack of a water treatment facility in Pinellas County, Florida. These examples underscore the need to consider political risk today as something that impacts not just for-profit companies, but organizations of all types (i.e., profit, non-profit, public, quasi-public, private, etc.).

In order to accommodate both modern and emerging threats in the cyber realm as they pertain to different organizations, for purposes of this paper, political risk is

re-defined as: the possibility that an action by a governmental or non-governmental entity, regardless of motive, will impact an organization (i.e., profit, non-profit, public, quasi-public, private, etc.), positively or negatively. While in many cases the motivation of the risk generator may be political, it does not have to be. In these latter cases, political risk arises because the governance systems in place are unable to secure and protect an organization and its assets.

4.3 Uniquely critical: Cyber attacks & the electrical sector

In 2021 Jacquelyn Bualo and the tech-review firm TechJury.net shared startling findings regarding the number of cyber-attacks that occurred globally throughout the previous year. For instance, they determined that ransomware attacks grew by 150%, while around the world 30,000 web sites were hacked daily. In addition:

- 64% of companies worldwide have experienced at least one form of a cyber-attack
- There were 20M breached records in just March 2021
- Every 39 seconds, there is a new attack somewhere on the web
- Approximately 24,000 malicious mobile apps are blocked daily on the internet

Amongst the many industries vulnerable to these growing attacks is the energy segment. This is why many industrialized nations, including the U.S., categorize energy as a critical infrastructure sector (for a complete list, see box below). According to Presidential Policy Directive 21 [PPD-21], critical sectors are defined as those whose "assets, systems, and networks . . . are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety or any combination thereof (16 Critical Infrastructure, NDA)."

16 critical infrastructure sectors in the U.S.[2]

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector

2 Similarly, in its April 2021 "Annual Threat Assessment" the U.S. Office of the Director of Intelligence (ODNI) cautioned that countries like China have the capacity to "launch cyber-attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States (Annual Threat, 2021; Miller 2021)."

5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector (whereas sector includes electricity, oil, and natural gas segments)
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Water and Wastewater Systems Sector

The CISA's assessment is supported by the World Economic Foundation (WEF) who in their 2020 Global Risks Report listed cyber-attacks on critical infrastructure sectors, including energy, as the fifth top risk (Granados, 2020).[3]

Unlike most other sectors, however, energy is not only described as vital but "uniquely critical" to the extent that it enables most of the other critical sectors (16 Critical Infrastructure, NDA). If power were disrupted for a long period of time over a large swath of the nation, it could have a cascading impact because almost all of the other critical systems would be negatively impacted including communications, financial, information technology, transportation, water, etc. This helps explain why the three segments that make up the energy sector – electricity, oil, and natural gas – are among the most frequent targets of and uniquely vulnerable to cyber-attacks. As Gib Sorebo et. al. (2020) write, cyber-attacks on critical infrastructure are always a serious threat, but particularly when it comes to the electricity sector because of the potential for "devastating cascading effects" which can result in "loss of life, economic costs, and industrial disruption, among other severe consequences."

This is not just supposition. In their study of cyber risk in the electric power grid, Steven Livingston et al. (2018) notes that the U.S. energy grid has become one of the three most targeted sectors for cyber intrusion. According to a 2016 report of incidents by sector, twenty percent of the reported attacks in the United States that year were against the energy sector (National Cyber Security, 2016). Speaking before a House Appropriations subcommittee in early 2018, then Energy Secretary Rick Perry placed the number of attempted attacks at "hundreds of thousands" per day (quoted in Siegel, 2018). The remark prompted a top Democrat on the Senate Energy Committee, Sen. Maria Cantwell (WA) to urge the federal government to do more to

3 Similarly, in its April 2021 "Annual Threat Assessment" the U.S. Office of the Director of Intelligence (ODNI) cautioned that countries like China have the capacity to "launch cyber-attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States (Annual Threat, 2021; Miller 2021)."

protect the U.S. power grid. “Our energy infrastructure is under attack,” Cantwell said. “it’s under cyberattack and we need to do much more to protect it as a national critical asset (quoted in Siegel, 2018).”

Throughout the COVID-19 pandemic, the threat of cyber-attacks on critical infrastructure, particularly the electricity grid in the U.S. has only increased. As Manny Cancel, senior vice president of the North American Electricity Reliability Corporation (NERC) and CEO of the Electricity Information Sharing and Analysis Center (EUSAC) said, the sector saw an “unprecedented” increase in cyber threats during the pandemic (quoted in Miller, 2021). He attributed the increase to the fact that actors from nation states to cyber criminals were growing increasingly capable of launching such attacks, and that throughout the pandemic, an increasing number of employees in that sector were working from home (Miller, 2021). Cancel’s assessment of the vulnerability of the sector was underscored by a General Accounting Office (GAO) report released in early 2021 which concluded that the:

> U.S. electricity grid's distribution systems – the parts of the grid that carry electricity to consumers – are becoming more vulnerable to cyberattacks, in part because of the introduction of and reliance on monitoring and control technologies (Electricity Grid, 2021).

The report went on to note that while the U.S. Department of Energy is working on the energy sector portion of the national cybersecurity strategy, it has focused its efforts on the grid’s generation and transmission, as opposed its distribution systems. According to the GAO report, the “potential impacts from such attacks” is still “not well understood (Electricity Grid, 2021).”

This sector is not just increasingly under attack in the U.S., but around the world. A 2021 Cyber Threat Ranking Table from Hiscox, for instance, found that the energy sector in the United Kingdom was the most at risk of a cyber-incident (The Hiscox, 2021; Hurst, 2020). This comports with findings from other nations over the last several years. In the 2016 Threat Report by the Australian Cyber Security Centre (ACSC), the energy sector was identified as the area with the highest number of reported cyber incidents with 18 percent reported, as compared the next largest sector – banking and financial at 17 percent, followed by communications at 12 percent (Frewin, 2017).

As Table 4.1 shows, in the last decade, cyber-incidents impacting the energy sector have been reported world-wide including Australia, the European Union, Iran, Japan, Saudi Arabia, the Ukraine, United Kingdom, and the United States, just to name a few (Sorebo et al., 2020).

Perhaps the most well-reported of these were the two separate information technology [IT] and operational technology [OT] cyberattacks in the Ukraine. In December 2016, hackers infiltrated an electric transmission station north of Kiev and successfully blackened out about one-fifth of the capital’s total power (Greenberg, 2017). This was the second such attack on the Ukraine’s power grid. The first, that occurred a year earlier, caused power outages at three regional electric power distribution

Table 4.1: Sample of Cyber Incidents Impacting the Energy Sector Around the World (2009–2020).

2010	Iran	Stuxnet affects centrifuge control systems, causing malfunction, destruction and significant political consequences
2012	Saudi Arabia	Shamoon virus shut down 30,000 control systems, erasing data on hard drives and causing severe damage
2014	United States	Brute-force attack used to hack passwords on utility network
2015	Ukraine	Black Energy attack on Ukraine energy companies left 225,000 citizens without power
2017	European Union	Virtual wiretapping of unencrypted traffic from transmission operator in UK passing through routers in Northern Ireland and Wales
2017	Saudi Arabia	Trisis/Triton penetrated the safety systems of a petrochemical plant to sabotage operations and trigger an explosion
2019	United States	Firewall firmware vulnerabilities used to cause denial of service attacks, affecting utility control center
2020	European Union	Ransomware attack strikes large utility, supposedly stealing 10 TB of sensitive data, with a threat to expose it if not paid a ransom

Source: Adapted from Sorebo et al, 2020, p. 5, Figure 1; Livingston et al, 2018, p. 4

companies (Oblenergos) and impacted approximately one-quarter of a million customers who were left without power for hours in the middle of the winter (ICS Alert, 2016). Those attacks, which U.S. and other cyber security experts have attributed to Russia, were noteworthy because they "set an ominous precedent for the safety and security of power grids everywhere (Zetter 2016)." After the second attack, ESET Security Research Robert Lipovsky argued, "If this is not a wakeup call, I don't know what could be (quoted in Greenberg, 2017)."

As Lipovsky noted, the Ukrainian shutdowns showed the world just how vulnerable this sector is to actors with the skills to mount cyber-attacks (Greenberg, 2017). Tucker Bailey et. al., highlights three characteristics that help explain why the electrical power sector is uniquely vulnerable to cyber-threats. First, is the increase in the number and type of actors focused on mounting cyber-attacks against utilities for a variety of reasons. This includes, but is not limited to nation-states, organized criminals, hacktivists, and individual hackers. Second, the utilities "attack surface" is not only large but increasing as a result of their geographic and organizational complexity, as well as the "decentralized nature of many organizations' cybersecurity leadership (Bailey, 2020)." A fact that harkens back to the definition of political risk being intimately related to an absence or failure of governance. Finally, and not widely discussed, is the fact that this sector contains the rare interdependency between the physical and cyber infrastructure that leaves the organizations that control them particularly exposed (Bailey, 2020). These factors, coupled with the

exposure during the pandemic noted by Cancel, and the increasing number of actors with the skills, interests and capabilities of launching these types of attacks, leave the electricity segment of the energy sector uniquely vulnerable.

4.4 Research design & method: Using content clouds to sample 10-K filings

Content Clouds as a Method of Exploratory Qualitative Data Analysis With this understanding of the increasing risk cyber-attacks pose to a sector that is defined as both uniquely vulnerable and critical, this study sets out to measure how seriously those who control the electricity segment in the U.S. take this threat. Where does it rank in comparison to other threats these organizations face? Do the people in charge of the companies that run the electric grid identify cyber-attacks as a serious threat to their core business practices as we are often led to believe?

In order to address these questions, this chapter relies on an unobtrusive method of exploratory qualitative data analysis and visualization via the creation of content clouds. Julie Cidell's (2010, 514) describes the use of content clouds as "a type of visualization that summarizes the contents of a document by depicting the words that appear most often in larger, darker type within the cloud." While Cidell's work is focused on geography, the use of this method as a form of qualitative data analysis makes sense across multiple disciplines because content clouds provide a useful way to summarize and compare information from a host of documents. Moreover, any material that can be examined using content analysis can be visualized through the generation of content clouds.

As Cidell (2010) notes, this approach is particularly useful when the research is exploratory and inductive. While there has been a good deal of research in the areas of cyber- attacks and cyber-risk, there has been significantly less examination when it comes to the specific questions at issue in this study. Given the amount of attention cyber threats have generated in the press of late, there is a gnawing supposition that those operating critical infrastructure sectors would take it seriously; but just how seriously and how it compares to other threats they face and other risks to their business operations is yet unknown. As a result, this inductive and exploratory approach is advisable in that it allows for investigation without expectation and hypothesis. Rather than presupposing answers to the research questions, this study begins at the bottom of the research circle with the data and based on the findings, induces an explanation or theory to make sense of the findings.

The web site FreeWordCloudGenerator.com was used to generate the content clouds for this study. It is one of a number of cloud generators, but chosen because it was free for noncommercial use. It removes (or allows for inclusion of) stop words, numbers, and special characters, while providing an ease of use for simple

visualization projects. It allows for visualization of files larger than 500 kilobytes which was necessary given the size of the Risk sections of the 10-K filings for the companies included in this sample.

Content: 10-K Filings in the U.S. publicly traded companies are required by the Securities and Exchange Commission (SEC) to file 10-K reports.[4] These annual reports are designed to help keep investors informed of a company's financial performance, as well provide them with the time and information they need to make investment decisions. This legal requirement was initially part of the Securities Exchange Act of 1934 but has been amended over the years. In 2004, the SEC passed the "Final Rule" which gave corporations 75-days, as opposed to the original 90-days, after the end of the fiscal year to file their reports. This was the case for any company issuing shares available for public trade (Public Float) of at least $75 million; those with over $700 million in public float only have only 60-days to file.

A typical 10-K filing includes several sections that focus on an overview of the company's main business operations, products, and services, select financial data, management decisions and analysis, financial statements, supplementary data and most critical to this study, risk factors. This last section, generally included in SECTION 1A, was made mandatory by the SEC in the mid-2000s in order to ensure that investors and shareholders are aware of risks facing the company with the understanding that this was critical to making investment decisions. The SEC determined that if an investor is to take a risk and invest in a company, they are entitled to know all potential risks facing the organization in the near future.

Sample The risk portion (1A) of the last set of 10-K filings of a sample of electric companies in the U.S. was used in an effort to determine where cyber-attacks rank in the context of risks facing these organizations. In order to determine which companies would be included in the sample, MergentOnline.com was used. MergentOnline offers a good deal of data on companies and corporations across the world. As their web site notes, this includes "company financials, descriptions, history, property, subsidiaries officers and directors" among much else. Using Mergent's advanced search function, I was able to isolate active U.S. utility companies. By specifying the Industry Classification Benchmark (ICB) code 65101015, I was able to identify the sixty-nine (69) listed as "conventional electricity utilities." Based on this list, I sampled more than a quarter (26%) of the Risk sections (1A) of their latest 10K filings (February 2021, for the Fiscal Year ending December 31, 2020). These filings were found via either MergentOnline or the SEC's Edgar search engine (https://www.sec.gov/edgar/search/).

4 The U.S. is not unique in requiring this type of filing, other countries require similar type of information to be made publicly accessible as well. In the United Kingdom, for instance, since 1844 the Companies House has listed financial information. In Canada the System for Electronic Document Analysis and Retrieval (SEDAR) is used to ensure investors' awareness. Similar systems are used in countries worldwide, including Belgium, China, and Germany, among many others.

Table 4.2: Conventional Electricity Companies Sampled (U.S., Public, Active, 2020).

Company Name	SIC Code	Exchange	Ticker	Customers (M)	Employees	Revenue ($B)	Shareholders
AES Corp	4911	NYS	AES	2.5	8,200	10	3,771
Allete Inc	4931	NYS	ALE	185,000**	1,322	1	20,000
Alliant Energy Corp	4931	NMS	LNT	1	3,375	3	23,282
Connecticut Light & Power	4911	NBB	CNLT N	1.2	1,381	4	1
Consolidated Edison Co. NY	4931	N/A	N/A	3.4	12,477	11	N/A
Consumers Energy Co.	4931	NYS	CMS PRB	2	7,617	6	1
Dominion Energy Inc	4911	NYS	D	7	17,300	15	130,000
DTE Energy Co	4911	NYS	DTE	3.5	10,600	13	47,485
Edison Intl/Southern Cal Edison	4911	NYS	EIX	14	13,351	14	27,353
Entergy Corp	4911	NYS	ETR	2.7	13,400	11	22,817
Exelon Corp	4931	NMS	EXC	10	32,340	34	91,240
NextEra Energy/FPL	4911	NYS	NEE	5.6	14,000	17	16,080
PG&E Corp	4931	NYS	PCG	16	24,000	19	46,536
Public Service Enterprise Group Inc	4911	NYS	PEG	2.3	12,788	10	54,220
Southern Co.***	4911	NYS	SO	8.54	27,700	21	107,362
Tennessee Valley Authority	4911	NYS	TVC	10	9,989	10	N/A
Virginia Electric & Power	4911	NL	N/A	2.4	6,000	8	1
Xcel Energy	4931	NMS	XEL	5.8	11,367	12.3	52,689
				97.95	227,207	219.3	642,838

*All data expressed in these columns are approximations/estimations, rounded, and based on publicly available data & company filings

**in thousands

***Holding Company, holding company provides electric service to customers in 3 Southern states via is subsidiaries (Alabama Power Company, Georgia Power Company, and Mississippi Power Company, Co.)

Source: Compiled from information publicly available and accessible on MergentOnline

A complete list of the conventional electricity companies sampled for this study are included in Table 4.2. The sample includes some of the largest public and active electric utility companies in the U.S. as measured by revenue and number of customers, as well as a geographic cross-section.[5] In total, in 2020, the 18 companies sampled serve approximately 97.95 million customers, employed over a quarter of a million people, and generated roughly US$219B in revenue.

4.5 Findings

Do Cyber-Attacks Make the Risk Section? An Aggregated View. It is difficult to determine how seriously the largest electric companies in the U.S. are taking the threat of cyber-attack. One measure, may be the amount of money companies are spending, per year, on protection. Another example, reflected in this study, is how prominently the threat is featured in their 10-K filings in comparison to other risks. If these organizations are taking the threat as seriously as many experts today suggest they should, it stands to reason that it would be featured prominently in the Risk sections of their 10-K filings. In order to make this determination, the Risk (1A) section of the last 10-K filings (2021) of each of the companies sampled was examined and compiled into a content cloud.

Figure 4.1 shows the content cloud portrays the general pattern of what risks matter most to the sample of 10-K filers included in this study. The words that appeared most often in the risk portion of their 10-k filings are displayed in larger, darker type. In this instance, the top fifty (50) words are included.

In total, 5,389 distinct words were used in this portion of these filings. As Table 4.3 shows, the top ten terms used were: operations, financial, costs, energy, results, including, utility, business, facilities, gas. Across the filings, these terms were used between 534 and 954 times. As we continue further down the list to include the top-25 words used, the remainder include power, results, companies, customers, generation, impact, affect, ability, risks, operating, capital, regulatory, subject, nuclear, and condition.

Notably, as Figure 4.1 and Table 4.4 show, none of the terms associated with cyber threats, attacks, or ransomware made it into the top 50 of the most frequently used terms.

While cyber-risk related terms do appear, they do so with far less frequency and much further down the list than other words. As Tables 4.3 & 4.4 show, 'cyber' related terms not only failed to make the top 50 most-used terms, but they do not even make the top 150. 'Cyber' is the only term to crack the top 450 in fact, coming

5 The sample includes 9 of the 10 largest utility companies by revenue, 2014; as well as a sample of the leading electric utilities based on number of customers, 2019 (Leading Electric, 2021).

Figure 4.1: Content Cloud aggregated of Risk Section of 10-K Filings of 18 U.S. Electrical Companies.

Table 4.3: Most Frequently Used Words in Risk Sections of 10-K Filings Sampled.

Ranking (#)	Frequency (N)	Word
1	954	Operations
2	908	Financial
3	829	Costs
4	742	Energy
5	664	Results
6	604	Including
7	601	Utility
8	597	Business
9	553	Facilities
10	534	Gas
11	531	Power
12	521	Result
13	489	Companies
14	485	Customers
15	470	Generation
16	465	Impact
17	462	Affect
18	462	Ability
19	456	Risks
20	455	Operating
21	455	Capital
22	443	Regulatory
23	402	Subject
24	393	Nuclear
25	389	Condition

Table 4.4: Placement and Frequency of Cyber-Attack Related Words (and their variants) Used in Risk Sections of 10-K Filings Sampled.

Ranking (#)	Frequency (N)	Word
178	106	cyber
472	42	Cybersecurity
1449	9	Cyberattacks
1657	7	cyber-attacks
2351	4	Ransomware
2702	3	Cyberattack
3312	2	Cybercrime
3581	2	cyber-security

in at 178 on the list with 98 mentions across the aggregated filings. This was followed much later by 'cybersecurity' (and its variant, 'cyber-security') which are used 44 times (ranking 472 and 3581 respectively).

Much further down the list are 'Cyberattacks' (and its variants 'cyber-attacks' and 'cyberattack') which are used a total of 19 times. While ransomware attacks on utilities have become common place, as it pertains to risks faced by these electric companies, it was mentioned only 4 times in the context of Risk across all eighteen filings making it 2351 on the list. Likewise, the word 'cybercrime' was used only twice.[6]

A Similar Pattern at the Individual Level Figure 4.2 shows the content clouds for a sub-sample of five corporate filings mapped by approximate size (as measured by customer base). The general pattern of most frequently used words varies across the risk sections of these filings [see Table 4.5]. Despite this, there are two terms that appear in the top 10 of all five of these filings – 'financial' and 'operations'. This is followed by the term 'costs' which appears in the top 10 of three of the filings (PG&E, Southern, and Exelon). While not in the top-10, the term also ranks high in the other two filings, coming in the top-25 for TVA (ranking 22) and the top-20 for NextEra (ranking, 16).[7]

As in the case of the aggregated data filings, when examined individually, the sub-sample demonstrates little concern or discussion of cyber-threats. As Table 4.6 shows, the two most frequently used cyber-threat terms across the sub-sample were 'cyber' (used 27 times in total) and 'cyber-security' (used 15 times in aggregate).

6 Other key terms checked did not appear, for example the common 'distributed denial of service (s)' or 'ddos'.

7 If combined with the variant 'cost' in all cases, the frequency of usage increases a good deal. This is also true for the other words reflected as the data mapping software does not combine those in the calculation.

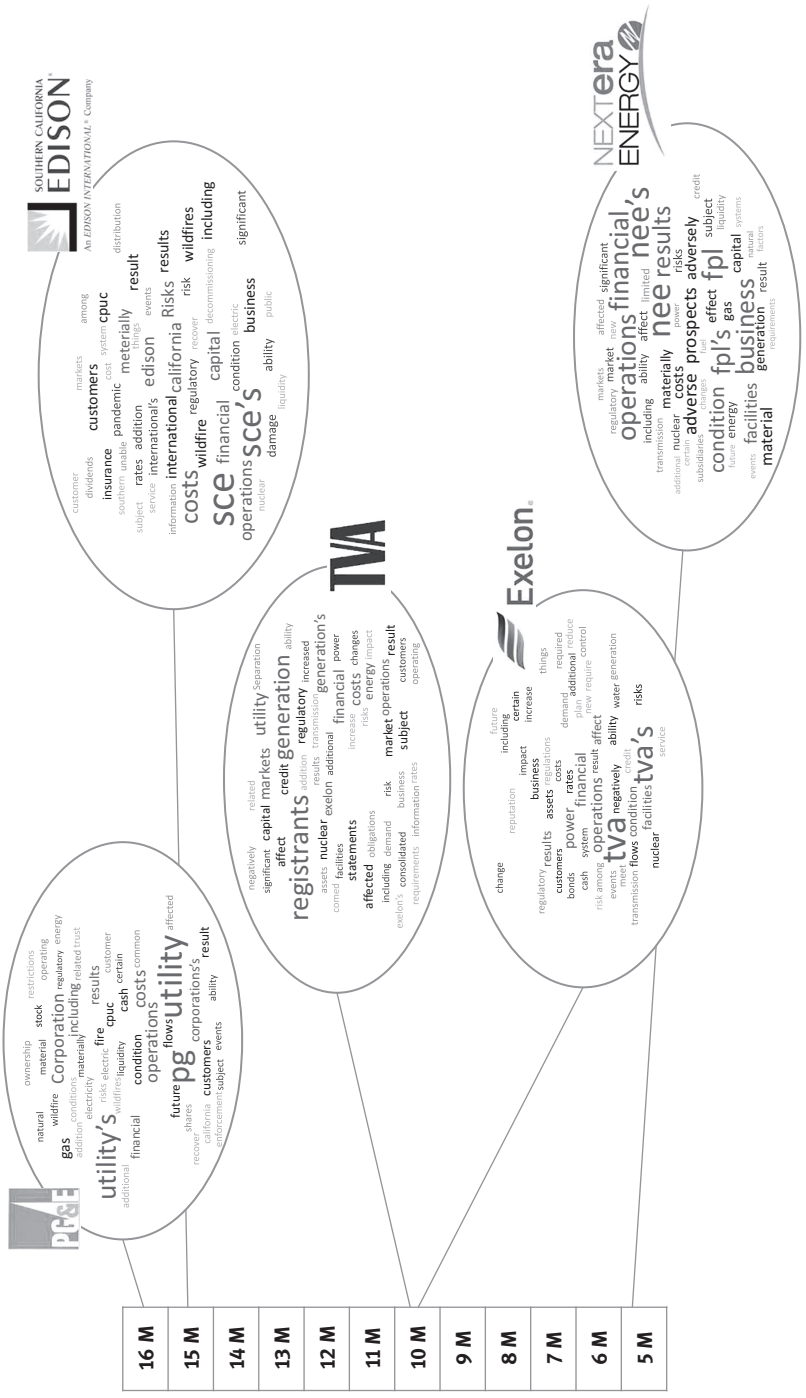

Figure 4.2: Content Clouds of Risk Section of 10-K Filings of a Sub-sample of Electrical Companies.

Table 4.5: Most Frequently Used Words in Risk Sections of a Sub-Sample of Electrical Companies.

Ranking (#)	PG&E	Southern	TVA	Exelon	NextEra
1	utility	Sce	tva	registrants	nee's
2	pg	sce's	tva's	generation	nee
3	utility's	***Costs***	**operations**	utility	fpl
4	corporation	Edison	power	**financial**	fpl's
5	***costs***	**financial**	**financial**	***costs***	**financial**
6	corporation's	Risks	results	generation's	**operations**
7	**financial**	**operations**	condition	exelon	business
8	**operations**	california	facilities	markets	results
9	including	materially	cash	energy	condition
10	results	capital	affect	**operations**	facilities

Table 4.6: Frequency (#) of Cyber-Attack Related Words (and variants) in Risk Sections of Sub-sample.

	cyber	cyberattack(s)/cyber-attack(s)	ransomware	cybercrime/ cyber-crime	cybersecurity
PG&E	9	2	0	0	0
Southern	6	0	1	0	6
TVA	8	0	0	0	4
Exelon	2	1	0	0	5
NextEra	2	4	0	0	0
Total	**27**	**7**	**1**	**0**	**15**

Interestingly, the term 'ransomware' only occurred once in this section of the risk filings sub-sampled (Southern California/Edison), while 'cybercrime' and its variants were not used at all.

Not Even Lip Service In the wake of the Colonial attack, many security experts said that at the very least, they hoped it served as a "wake-up call." As Tobias Whitney argued, it is more important than ever that those working in critical infrastructure sectors are taking these threats seriously and not just paying "lip service to these issues (quoted in Miller, 2021)."

The findings of this study do not allow us to conclude whether the electrical companies sampled are taking the threat seriously. They do, however, show that cyber threats are not prominently featured as a risk to their organizations in their most recent 10-K filings. To this extent, the findings suggest that the situation is even worse than Whitney may have imagined. Far from paying lip service to the issue, the electric companies hardly even mention the threat of cyber-attacks – at least not in the risk sections of their 10-K filings. Given how much these issues are in the public consciousness this year, the results are astounding.

If cyber threats and ransomware attacks are as existential a threat to the U.S. as we are often told, and if electrical sector is indeed both uniquely vulnerable and critical, one would hardly know it based on a reading of their latest 10-K filings. Few people would imagine that in 2021, the term ransomware would be mentioned only four times in the risk sections of the 10-K filings of the U.S.'s largest electrical companies sampled for purposes of this study. Instead of cyber and ransomware, the risks that are the focus of these companies' attention are financial, operations, and costs.

Inducing an Explanation for the Findings In the wake of the pipeline attack, President Biden established a DOJ cyber-security task force to investigate the growing number of attacks and in particular the risks posed to America's critical infrastructure. During a June 2021 news briefing, task force Deputy Director Lisa Monaco spoke in no uncertain terms about the danger cyber and ransomware threats present to those in critical infrastructure sectors:

> the threat of severe ransomware attacks pose a clear and present danger to your organization, to your company, to your customers, to your shareholders, and to your long-term success. So, pay attention now. Invest resources now. Failure to do so could be the difference between being secure now, or a victim later (quoted in "Justice Department," 2021).

This type of stark warning came just a few months after most of the electrical companies sampled in this study submitted their latest filings to the SEC. While it is difficult to know why these organizations did not highlight these risks, one possibility is that these filings reflected fiscal year 2020. Perhaps, the 2021 attacks have served as a wake-up call and future research may find that the filings next year differ substantially from their predecessors in this regard.

Another possibility is that the Risk sections of the 10-K are viewed as a place to focus on financial as opposed to other types of risks. It may be strange, particularly given the amount of ransom asked in the Colonial and JBS hacks, to imagine that these companies do not see the attacks as a potential financial risk. One reason for this may be the recent growth in cyber liability insurance. The research firm AdvisorSmith found that in 2020, U.S. businesses with cyber insurance paid an average annual premium of $1,485 (Pattison-Gordon, 2021). While more research needs to be done in this area, it may be that this type of investment substantially diminishes the amount of financial risk a company may sustain during an attack; to this extent, if they see the Risk section of the 10-K as a place to discuss major financial risks, premiums of this level, may be an indication as to why ransomware attacks are not seen as a major financial risk, particularly when compared with other threats facing these companies.[8]

8 It is also worth noting that some clarification may be in order from the SEC regarding what types of risks are appropriate for this section of the 10-K.

4.6 Conclusion

Traditional conceptions of political risk tended to focus on the risks to "for-profit" companies. An earlier section of this paper referenced the need to broaden this view to include public entities, quasi-public entities, public, and non-profit organizations. This is underscored in the case of cyber and ransomware attacks on electrical companies and other critical infrastructure in the U.S. As cyber insurance options continue to grow and more organizations take advantage of them, it is possible to imagine that while disruptive in the short term, these attacks do not pose as much risk to these organizations as other types of threats (i.e., regulation). Despite the recent media narrative, these organizations are cognizant of the major risks they are facing, and as disruptive as cyber-attacks may be, they do not rise to the top.

Viewed from another perspective, when focusing on the electrical companies, we are looking at the wrong organization to begin with. The industries most at risk when it comes to cyber and ransomware attacks on critical utilities are not private companies, but the public entities, governments, and quasi-governmental organizations. These entities are charged with serving and protecting the public's health, safety, and well-being, as well as the protecting state/nation from internal and external attack. These are their top priorities, whereas the primary responsibilities of the electrical companies differ substantially. And in the 21st Century, this goal cannot be accomplished sans a fully functioning grid. In their 2020 report on how best to deter attacks against the electrical grid, Anu Narayanan et al. underscored just how essential it is to U.S. national security that the grid be secure:

> The U.S. Department of Defense (DoD) increasingly relies on electric power to accomplish critical missions. As a result, ensuring that forces and facilities have access to a reliable supply of electric power is critical for mission assurance. However, DoD does not directly manage its supply of power; most of the electricity consumed by military installations in the continental United States comes from the commercial grid – a system that is largely outside of DoD control and increasingly vulnerable.

Defense and security are critical, but only one reason that disruptions of the grid presents such a serious threat to the public sector – from the U.S. federal government to all state, county and local governments. Imagine, the threat posed to the country by a massive, coordinated attack that took down the grid for a substantial period of time. During a 2015 hearing before the Senate Committee on Homeland Security, former Central Intelligence Agency Director James Woolsey explained the potential impact in stark terms. When asked by Chairman Ron Johnson (WI) to "describe what happens to society when the grid is down for [a] very long time (quoted in "Protecting" 2015)?" Woolsey said:

> There are essentially two estimates on how many people would die from hunger, from starvation, from lack of water, and from social disruption. One estimate is that within a year or so, two-thirds of the United States population would die. The other estimate is that within a year

> or so, 90 percent of the U.S. population would die. We are talking about total devastation (quoted in "Protecting" 2015).

The ninety percent death estimate is based on a 2008 government study and the threat from this type of attack has only increased since that time. Based on this scenario, when we reference the political risk of cyber and ransomware attacks, it is important to look at not just the risk from the perspective of the electrical companies, but public sector organizations such as the federal government, the CIA, Homeland Security and the states agencies. It is these organizations – not the electrical companies themselves, whose top priority is to protect the health, safety, welfare, and well-being of citizens. Do the electrical companies face risk as a result of these attacks? Absolutely, but the degree of risk differs. The fact is that cyber and ransomware attacks may not be at the top of their priority list when it comes to risks being addressed. In the case of the public sector, the risks are more substantial.

In *Political Risk,* Rice et al (2018b, 192–195) provides a framework for understanding the differential nature of these risks. In their discussing of risk mitigation, the authors note that prioritization is key to mitigating risk. Since no organization can protect itself against all risks, mitigation requires understanding (a) what assets are most valuable (i.e., what are their priorities), (b) what assets are most vulnerable, and (c) focusing attention on the highest value assets that are most vulnerable. As Table 4.7 shows, this is the quadrant labeled 'top priority' where the most vulnerable and most valuable assets intersect.

Table 4.7: Rice et al Matrix of Value & Vulnerability.

	Lower Vulnerability	**Higher Vulnerability**
Lower Value	Low priority	Medium priority
Higher Value	Medium priority	**Top priority**

Source: Rice et al, 2018b, p. 195

If we apply this matrix to the electrical companies, it is possible that their understanding of the most valuable and vulnerable assets does not place cyber and ransomware attacks in the top priority quadrant. In the worst-case scenario, they can be insured to survive a widespread attack. The same cannot be said of the threat from extreme weather. The Texas blackout that occurred during the winter of 2021 was just another example in a long line of reminders that climate-driven, extreme weather is increasingly putting stress on the U.S. power system and much needs to be done to ensure that the power grid can withstand extreme weather events which will become more common place in the future. Several months later, in the wake of another summer of devastating wild fires on the West Coast, Pacific Gas and Electric Company, the largest natural gas and electric utility in the U.S. which serves 16

million people in Northern and Central California, announced that it was planning to bury 10,000 miles of power lines at an estimated cost of $20 billion (Blunt, 2021). As we reflect on what might be included in the utilities "high priority" quadrant, these types of concerns likely make the list.

In contrast, public entities such as the Department of Defense or City of New York, have very different priorities and vulnerabilities which, as a result, may make these types of attacks a key priority. In the case of the latter, public safety and health are among the city's top priorities and given how vulnerable the grid is to attacks and the devastating consequences that might ensue, these types of attacks become a top priority.

While this is a new area for exploration, future research might consider in future filings whether electrical companies and other utilities should begin to identify these types of attacks a more prominent feature? Alternatively, it would be important to gain a better understanding of the nature of the risks they feel are important to cover in these filings (i.e., merely financial for instance?) They should also do a comparison of the Value/Vulnerability Matrices for utility companies versus public/quasi-public sector organizations. If the political risk of cyber-attacks is greater for public versus private entities, then it is incumbent on the government to take the necessary steps to ensure that those commercial entities charged with managing our energy supply are regulated to a degree that they are required to pay more than just lip service to this threat.

References

"16 Critical Infrastructure Sectors." (NDA). *Cybersecurity and Infrastructure Security Agency (CISA). Identifying Critical Infrastructure During COVID-19 | CISA*.

"Annual Threat Assessment." (2021). "Annual Threat Assessment of the U.S. Intelligence Community." *Office of the Director of National Intelligence*. April 9, 2021. ATA-2021-Unclassified-Report.pdf (dni.gov)

Bailey, Tucker, Adam Maruyama and Daniel Wallance. (2020). "The energy-sector threat: How to address cybersecurity vulnerabilities." *McKinsey and Company*. November 3, 2020. The energy sector threat: How to address cybersecurity vulnerabilities | McKinsey.

Baker, Sinead. (2016). "FBI Director Christopher Wray compared the latest spate of ransomware attacks against the US to 9/11." *Yahoo News*. June 4, 2021. FBI Director Christopher Wray compared the latest spate of ransomware attacks against the US to 9/11 (yahoo.com)

Blunt, Katherine. (2021). "PG&E, in Reversal, to Bury Power Lines in Fire-Prone Areas." *Wall St. Journal*. July 21, 2021.

Bulao, Jacquelyn. (2021). "How Many Cyber Attacks Happen Per Day in 2021." TechJury. June 17, 2021. https://techjury.net/blog/how-many-cyber-attacks-per-day/

Cidell, Julie. (2010). "Content clouds as exploratory qualitative data analysis," *The Royal Geographical Society*. Vol. 42, No. 4. December 2010, pp. 514–523.

Deringer Heidi and Jennifer Wang. (1997). "Note on Political Risk Analysis." *Harvard Business School*. 9-798-022. September 17, 1997.

Electricity Grid. (2021). "Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems." *General Accounting Office (GAO)*, GAO-21-81. March 18, 2021. Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems (gao.gov)

Engemann, Kurt J. and Rory V. O'Connor, Ed. (2021). *Project Risk Management: Managing Software Development Risk*. Berlin: De Gruyter.

Frewin, Heath. (2017). "Protected Assets – Energy and Cyber Security." *Energy Insider*. Energy Networks Australia. February 23, 2017. Protected Assets – Energy and Cyber Security | Energy Networks Australia.

Goldbaum Christina and William K Rashbaum. (2021). "The M.T.A. Is Breached by Hackers as Cyber attacks Surge." *New York Times*. June 3, 2021. https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html

Granados, Emilio Franco. (2020). "The Global Risks Report." *Insight Report*, 15th Edition. World Economic Forum. WEF_Global_Risk_Report_2020.pdf (weforum.org)

Greenberg, Andy. (2017). "'Crash Override': The Malware That Took Down a Power Grid." *Wired*. June 12, 2017. Crash Override Malware Took Down Ukraine's Power Grid Last December | WIRED.

Hurst, Aaron. (2020). "Energy sector most at risk of cyber incidents, Hiscox analysis reveals." *Information Age*. October 14, 2020. Energy sector most at risk of cyber incidents, Hiscox analysis reveals (information-age.com)

ICS Alert (IR-ALERT-H-16-056-01). (2016). "Cyber-Attack Against Ukrainian Critical Infrastructure." February 25, 2016. *Cybersecurity & Infrastructure Security Agency* (CISA). Cyber-Attack Against Ukrainian Critical Infrastructure | CISA.

Javers, Eamon. (2021). "Here's the hacking group responsible for the Colonial Pipeline shutdown." *CNBC*. May 10, 2021. Hacking group DarkSide responsible for Colonial Pipeline shutdown (cnbc.com)

"Justice Department announces Seizure of Millions in Ransomware Paid to Colonial Pipeline Hackers." (2021). *Yahoo News*. June 7, 2021. https://news.yahoo.com/justice-department-announces-seizure-millions-160440847.html

"Leading Electric Utilities Based on the Number of Customers in the United States 2019." (2021). *Statista*. Largest U.S. utilities by number of customers 2019 | Statista.

Livingston, Steven, Suzanna Sanborn, Andrew Slaughter, and Paul Zonneveld. (2018). "Managing Cyber Risk in the Electric Power Sector." *Deloitte Insights*. DI_Managing-cyber-risk.pdf (deloitte.com)

Miller, Maggie. (2021). "Colonial Pipeline attack underscores US energy's vulnerability." *The Hill*. May 10, 2021. Colonial Pipeline attack underscores US energy's vulnerability | TheHill.

Narayanan, Anu, Jonathan William Welburn, Benjamin M. Miller, Sheng Tao Li, Aaron Clark-Ginsberg. (2020.) "Deterring Attacks Against the Power Grid." *Rand Corporation*.

National Cybersecurity and Communications Integration Center. (2016). FYI 2016 Incidents by Sector as reported in Livingston, Steven, Suzanna Sanborn, Andrew Slaughter, and Paul Zonneveld. (2018). "Managing Cyber Risk in the Electric Power Sector." *Deloitte Insights*, p. 2, fn. 4. DI_Managing-cyber-risk.pdf (deloitte.com)

Pattison-Gordon, Jule. (2021). "What Can Government Do as Cyber Insurance Costs Increase." *Government Technology*. July 14, 2021. What Can Government Do as Cyber Insurance Costs Increase? (govtech.com)

"Protecting the Electric Grid From the Potential Threats." (2015). Hearing Before the Committee on Homeland Security and Governmental Affairs, United States Senate, 114th Congress, S. Hrg. 114–483. July 22, 2015. U.S. Government Publishing Office. – PROTECTING THE ELECTRIC GRID FROM THE POTENTIAL THREATS OF SOLAR STORMS AND ELECTROMAGNETIC PULSE (govinfo.gov)

Rice, Condoleezza and Amy B. Zegart. (2018a). "Managing 21st Century Political Risk." *Harvard Business Review*. May–June 2018. https://hbr.org/2018/05/managing-21st-century-political-risk

Rice, Condoleezza and Amy B. Zegart. (2018b). *Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity*. New York: Hachette Book Group.

Searle, John R. (1993). "Rationality and Reason. What is at Stake?" *Daedalus*. Fall 1993. 122, 4. Searle – Rationality and Realism, What Is at Stake | Copyright Law | Law (scribd.com)

Shue, Craig. (2019). "Should Cities Ever Pay Ransome to Hackers?" *Wall St. Journal*. September 17, 2019. https://www.wsj.com/articles/should-cities-ever-pay-ransom-to-hackers-11568772120

Siegel, Josh. (2018). "Rick Perry boasts new cybersecurity office can handle Russian targeting of US grid." Washington Examiner. March 20, 2018. Rick Perry boasts new cybersecurity office can handle Russian targeting of US grid | Washington Examiner.

Sorebo, Gib and Thomas Duffey. (2020). "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors." *World Economic Forum*. July 2020. WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf (weforum.org)

The Hiscox Cyber Readiness Report, 2021. (2021). *Hiscox*. The Hiscox Cyber Readiness Report 2021 | Hiscox UK.

The SolarWinds Cyber-Attack. (2021). "The SolarWinds Cyber-Attack: What You Need to Know." Executive Overview. *Center for Internet Security*. March 15, 2021. The SolarWinds Cyber-Attack: What You Need to Know (cisecurity.org)

Uren, Tom. (2021). "Colonial Pipeline Cyberattack Exposes Serious Vulnerabilities." *The Maritime Executive*. May 27, 2021. https://www.maritime-executive.com/editorials/colonial-pipeline-cyberattack-exposes-serious-vulnerabilities

Viswanatha, Aruna and Dustin Vulz. (2021). "FBI Director Compares Ransomware Challenge to 9/11." *Wall St. Journal*. June 4, 2021. https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003?mod=e2twp

Walton, Robert. (2021). "Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, analysts say," *Utility Dive*. May 11, 2021. Colonial Pipeline hack highlights grid disruption risks even with IT-focused cyberattack, analysts say | Utility Dive.

Zetter, Kim. (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*. March 3, 2016. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED.