Security in the UK's Green Energy Supply Chain

CS4203 170002815 Word Count: 2977

30th September 2020

1 Introduction

1.1 Renewable Energy in the UK

The UK was the first major economy to announce a strive towards net-zero carbon emissions by 2050 [1] and 2019 saw renewable energy contribute for almost 40% of all power generation in the UK [2]. Market analysis shows that renewable energy in the UK is also a significantly superior investment to fossil fuel energy (+75.4% return compared to +8.8% return over 5 years) [3], which suggests green energy is likely to have a large economic expansion in the forthcoming years, with many new small and medium sized enterprises (SMEs) joining the effort.

In this report, the main security issues involved with the UK's green energy supply chain will be investigated, and recommendations will be given for SMEs already involved in the field, and those looking to join.

1.2 Security Issues Surrounding SMEs

According to the European Commission, an SME has a maximum of 250 staff and a maximum turnover of €50m [4]. The small number of staff often leads to no in-house security expertise and the small budget often leads to security being overlooked. A report by Ponemon Institute suggests that in 2018, only 63% of SMEs had an adequate budget for security, and 59% had in-house expertise [5].

Because of this lack of regard given to security, SMEs tend to suffer from frequent security attacks, with 61% of SMEs experiencing ransomware attacks at some point [5]. These attacks also tend to be successful, as 70% of the aforementioned ransomware attacks are paid and around 80% of attacks avoid any intrusion detection systems or anti-virus software the SMEs have in place [5].

Furthermore, the Ponemon Institute report suggests that not defending against security attacks correctly is costly. The average amount paid for a ransom is $1,466, and the average cost of a password compromise attack is $383,365 [5]. SMEs do not want to be paying this on a regular basis.

1.3 Security Issues Surrounding Supply Chains

SMEs involved in supply chains need to consider security, not only because of SMEs generally lack security measures, but also because supply chains are a increasingly popular targets for attackers [6].

The Shylock malware [7] and Dragonfly cyber-espionage group [8] are examples of where supply chains have been attacked in recent years through the abuse of the use of third-party software, and Chang, Su and Song's paper on shipping container security [9] highlights over 28 risks associated with maritime shipping. It can be seen from these examples that the use of third party software and maritime shipping pose great security threats - extrapolate this to other areas of supply chains and it is clear to see why organisations involved in the field should be strongly concerned with security.

1.4 Energy Supply Chain Considerations

The UK's green energy supply chain can be split up into two sections: the goods section and the energy section. The first section primarily involves the manipulation and transportation of physical goods for the development and maintenance of renewable power generation sites, and is represented by the left half of Figure 1. The second section involves the creation of energy at these sites, and its transmission and distribution to consumers - this is represented by the right half of Figure 1.

The goods section of the green energy supply chain involves security issues found in other supply chains. The transportation of goods is widely implemented and studied, allowing for smaller businesses to gather information on effective security measures. The paper by Chang et al. examines some security risks associated with maritime container shipping, and also offers advice and techniques for shipping companies, such as risk mapping [9].

The energy section of the supply chain contains security considerations that are not frequently found in other supply chains. Examples include the transportation and storage of electricity, where an attack could lead to loss of life, such as one which leaves hospital equipment unpowered. The UK energy supply chain also involves the transfer of data and funds between multiple institutions, which increases the importance of company cooperation to reduce risks. Security issues involving electricity, data and money are explored further in Section 4.

2 Literature & Background Review

As discussed in Section 1, the majority of SMEs have faced attacks, and there are numerous examples of supply chain attacks happening in the last ten years alone. Two examples are referenced in this report: the Shylock malware attack [7] and Dragonfly cyber-espionage group [8]. The cyber attack on Adobe in 2013 is used to express key topics in association with database usage [10] [11] - the two sources cover slightly different aspects of the attack, but both are relevant to this report.

Alongside these examples, technical and academic reports are discussed throughout this document. These include the Ponemon Institute report on cybersecurity in small- and medium-sized businesses in 2018, which interviewed over 1,000 SME employees. The other reports used are an academic report by Chang, Xu and Song on security issues relating to maritime shipping, and a technical report by Imperial College Business School's Centre for Climate Finance & Investment on the financial side of energy.

To supplement the other resources, Pfleeger & Pfleeger's *Security in Computing* is used to aid the analysis of security threats, and a variety of sources are used to state knowledge which is not assumed.

3 The UK's Green Energy Supply Chain

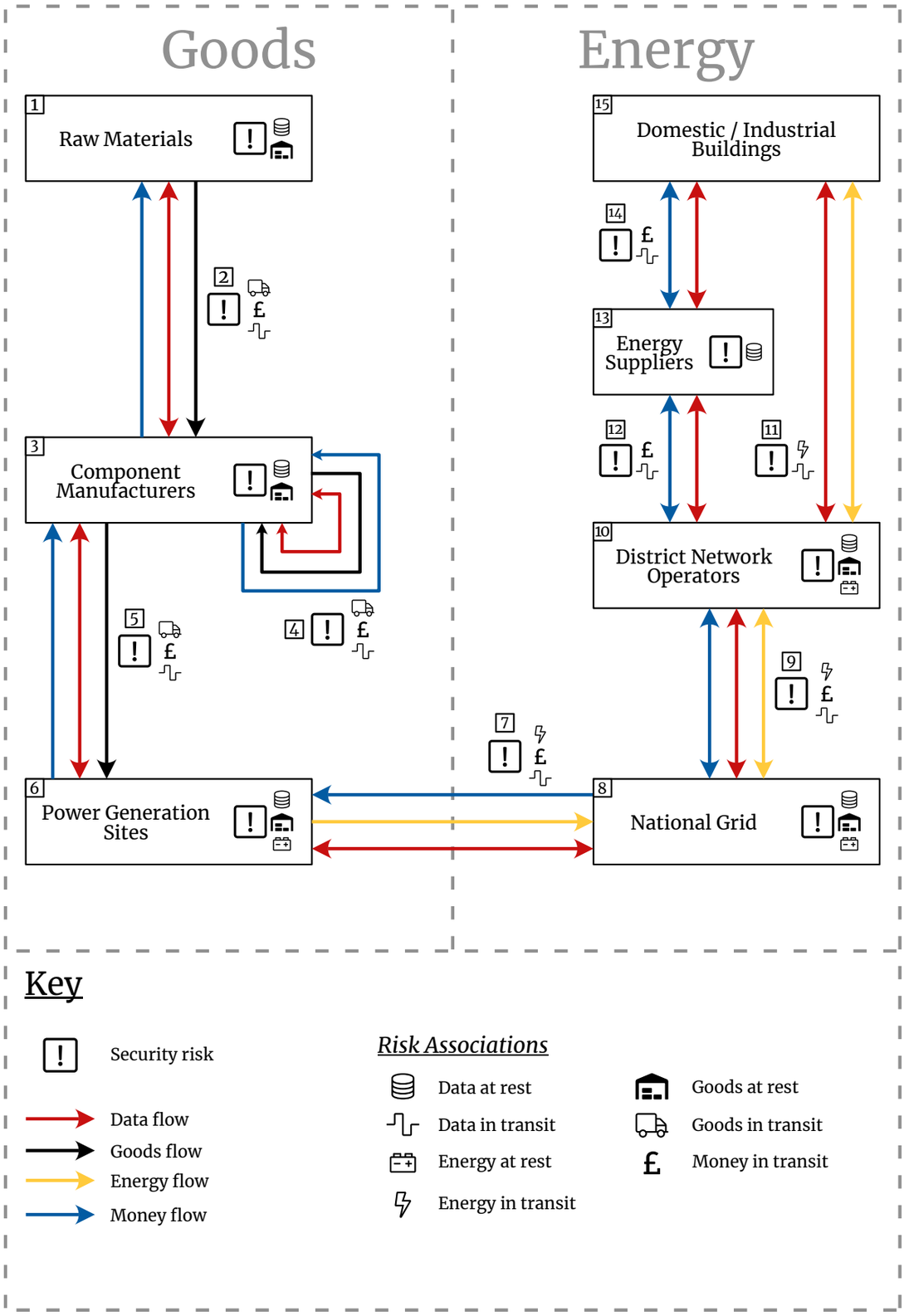

Figure 1: A broad overview of the UK's green energy supply chain and its associated security risks.

Figure 1 displays a diagram outlining the UK's green energy supply chain. The goods and energy sections are displayed on the left and right side of the diagram respectively.

The arrows in Figure 1 indicate the direction flow of goods, money, energy and data, and the colour of each arrow indicates which flow it represents according to the key. The exclamation mark bubbles represent one or more security risks, and the icons next to each exclamation mark bubble indicate what is generating the security risk(s), according to the key.

The numbers in Figure 1 start at *1* (Raw Materials) and end at *15* (Domestic / Industrial Buildings), incrementing as boundaries are crossed in an anti-clockwise fashion. The numbers represent the following situations:

1. **Raw Materials:** The acquisition, processing and storage of raw material.
2. **Goods Transportation:** The transportation of raw materials as goods between sellers and component manufacturers. This also involves the exchange of data between two or more companies, as well as the transfer of funds from manufacturers to raw materials suppliers.
3. **Component Manufacturers:** The manufacture and storage of components involved in renewable energy generation. Examples of these components include simple items such as screws to more specific items such as wind turbine blades.
4. **Goods Transportation:** The transportation of simpler components to manufactures of more complex components. An example of this is the transportation of screws from a screw manufacturer to a wind turbine blade manufacturer who use screws in their components. The goods and money arrows could flow both ways (e.g. RMA requests), however the general flow is represented in Figure 1.
5. **Goods Transportation:** The transportation of components from component manufacturers to power generation sites. These components are used directly in the development or maintenance of the sites. The goods and money arrows could flow both ways (e.g. RMA requests), however the general flow is represented in Figure 1.
6. **Power Generation Sites:** The sites at which renewable energy is generated, including wind farms or hydroelectric power stations. Energy is stored at these sites, and maintenance also occurs regularly.
7. **Energy Transportation:** The transportation of energy from generation stations to the energy transmission network (the National Grid). Green energy generated at UK power stations is sometimes passed directly to District Network Operators, but the majority is transported to the National Grid and is therefore the assumed path for energy in this report.
8. **National Grid:** The National Grid is the UK's largest high-voltage electricity transmission network which handles the transmission of the majority of UK-generated power [12].
9. **Energy Transportation:** The long-distance transportation of energy from the National Grid to District Network Operators, who may sell electricity back to the National Grid from areas with an energy excess, making this flow bidirectional.
10. **District Network Operators (DNOs):** Private companies who manage the distribution of electricity on a smaller, more focused scale than the National Grid. Examples include SP Energy Networks and Northern Grid. DNOs own equipment and infrastructure, and provide electricity to consumers, but payment is handled through energy suppliers (*13*).
11. **Energy Transportation:** The distribution of electricity from DNOs to homes and businesses. Microgeneration, such as from solar panel roofs, often leads to homes or businesses selling energy back to DNOs, making this flow bidirectional.
12. **Money Transfer:** The transfer of funds between energy suppliers and DNOs who buy and sell the rights to energy from each other.

13. **Energy Suppliers:** The customer-facing aspect of the UK's energy supply chain, including Octopus Energy and British Gas. They sell energy to domestic and industrial buildings, which is transmitted by the DNO. Consumers who partake in microgeneration often sell energy back to suppliers.
14. **Money Transfer:** The transfer of funds between consumers and energy suppliers who buy and sell energy from each other.
15. **Domestic / Industrial Buildings**: The consumers of green energy in the UK, who may also generate power.

4 Analysis, Discovery & Mitigation of Threats

4.1 Human-Oriented Threats & Risks

Humans are often the cause of security threats and attacks. Ponemon Institute found that in 2018 around 60% of data-breached SMEs located the root of the cause to be a negligent employee or contractor [5]. It is therefore crucial that systems are designed to reduce the number of human-oriented threats, and reduce the risk posed by ones which cannot be avoided.

The UK's green energy supply chain currently has many human-oriented security threats, some of the most prevalent are described in Table 1.

Table 1: Five human-oriented threats associated with the UK's green energy supply chain

Threat	**Location**	**Evaluation / Determination**	**Mitigation**
Password mishandling	Data at rest	Questionnaires & field studies	Enforce "strong" passwords. Use SSO & 2FA.
Incorrect operation of energy systems	Energy at rest & energy in transit	Manager observation & monitoring systems	Mandate training & ensure UIs are given adequate funding.
Incorrect usage of physical security systems	Energy at rest & goods at rest	Manager observation, field studies & monitoring systems	Use automatic security measures.
Couriers mishandling goods	Goods in transit	Field studies, questionnaires & data analysis	Mandate appropriate training, use suitable packaging & inform courier of relevant information on goods.
Database misuse	Data at rest	Risk assessment & verification software	Backup databases regularly, use multiple databases for redundancy & use the Principle of Least Privilege.

Pfleeger and Pfleeger's *Security in Computing* describes the three main aims of security as *confidentiality* (only authorised parties are able to access information), *integrity* (only authorised parties are able to modify information), and *availability* (authorised parties must be able to access and modify information) [13]. By using these aims to analyse the threats listed in Table 1, an insight is offered into why each of the rows represents a security risk.

The first row of Table 1 (password mishandling) could lead to the confidentiality, integrity and availability of data being compromised by an attack. Mandating the use of "strong" passwords, as suggested by NCSC [14], and a reliable password manager can reduce the risk posed by this threat. An alternative method is to alter the system's design; using a Single Sign-On (SSO) authentication scheme and/or Two-Factor Authentication (2FA) can reduce the impact of employees mishandling passwords. SSO allows software developers to focus on developing and testing a single high-quality and very secure authentication service instead of multiple less secure services. 2FA allows for security even if an employee's password is acquired by an attacker, as a second factor of authentication is required.

As well as row 1, row 5 of Table 1 could also lead to the compromise of confidentiality, integrity and availability. Both row 1 and row 5 are associated with data at rest, which can be found in 6 of the 15 situations within the supply chain diagram in Figure 1. To reduce the risk of database misuse, good database practice should be followed, including regular backups and duplicate databases to offer data redundancy - in the event of an attack, a company could recover by using a backup or rerouting to one of the duplicate databases, mitigating the majority of the effect of the attack. The Principle of Least Privilege should also be applied where possible when designing and developing databases to reduce unnecessary privileges and reduce the chance of network and computer exploits [15].

Rows 2 and 4 risk the availability of assets, however both have the potential to be mitigated by providing employees involved in these locations with the correct training. An example of this is transporting large wind turbine blades, which often requires specialised vehicles and can result in a great cost in damage if not completed correctly [16]. Row 4 (couriers mishandling goods) also risks the confidentiality of assets, however this threat is likely to happen more frequently than the other listed threats, and companies can therefore collect data and study it to analyse risks.

4.2 System-Oriented Threats & Risks

Although humans are most often the cause of security threats, the design of a system can also be a source of multiple risks. Table 2 lists some of the more prevalent system-oriented security risks associated with the UK's green energy supply chain.

Table 2: Five system-oriented threats associated with the UK's green energy supply chain

Threat	**Location**	**Evaluation / Determination**	**Mitigation**
Lack of information security during information flow	Data in transit	Verification software & consult security experts	Use encryption standard (e.g. RSA) & send only the required information.
Transmission of unnecessary data	Data in transit	Consult security experts & field studies	Avoid sending valuable information where possible & follow data regulations closely.
Inadequate physical security measures	Goods at rest & energy at rest	Consult security experts & risk assessment tables	Use security measures that use at least two factors of authentication & follow a security standard
Inadequate database security	Data at rest	Verification software & consult security experts	Follow a standard & use salting, encryption, zero-trust principles, etc.
Unnecessary idle goods	Goods at rest	Field studies, manager observation & data analysis	Deliver goods "just in time" & don't order excess goods.

By analysing Table 2 using Pfleeger & Pfleeger's aims of security, it is possible to see how each threat listed creates a risk to a supply chain's assets and why the consideration of a system's design and implementation is crucial to increase a supply chain's security.

Rows 3, 4 and 5 all risk the confidentiality, availability and integrity of assets. Row 3 (inadequate physical security measures) and row 5 (unnecessary idle goods) risk goods at rest by increasing the success rate of attacks and increasing the time window for attacks to take place on goods respectively. Using at least two of the three factors of authentication (e.g. a biometric scanner and a physical set of keys) can mitigate the risk caused by inadequate physical security measures, and using "just in time" delivery, where goods are delivered as close to the time that they are required as possible, can mitigate the risk caused by unnecessary idle goods.

Row 5 also offers an extra evaluation technique not necessarily available to the other threats - data analysis. Quantitative data on unnecessary idle goods can be gathered without the requirement of security attacks taking place; companies can take inventory of idle goods which are not needed and can dynamically alter the section of the supply chain providing the goods - this is something which can't be done with other threats, such as inadequate physical security measures.

The threat provided in row 4 of Table 2 (inadequate database security) may seem similar to the threat provided in row 5 of Table 1 (database misuse), however the mitigation techniques for the former need to consider the reduction in potential damage caused by an attack, but also the prevention of purposeful attacks from outside of the company, rather than just purposeful and accidental attacks from within the company. Salting and encryption, two of the mitigation suggestions in row 4 of Table 2, decrease the amount of meaningful information an attacker can gain from a database attack. Adobe suffered a database attack in 2013, where the usernames taken were not encrypted and the passwords were not hashed nor salted - this risked a lot more information being gathered by attackers than if the company had taken the proper precautions [10] [11].

Row 1 and 2 of Table 2 list threats to data in transit. It can be seen from Figure 1 that data in transit threats occur at every boundary crossing in the UK's green energy supply chain, suggesting that these threats need to be taken seriously. Information security during information flow (row 1) needs to be properly designed, implemented and tested, as if there is no encryption on data being sent, attackers can gain great amounts of meaningful information by completing a simple man-in-the-middle attack. Furthermore, a company sending unnecessary customer data, which it is responsible for, increases the risk of legal action being taken against that company - companies involved in the UK's complicated electricity supply chain should therefore take extra care when deciding which information to send to one another.

4.3 Other Threats & Risks

The threats and risks described in Sections 4.1 and 4.2 are very prevalent in the UK's green energy supply chain, however there are some other risks which should also be noted.

Figure 1 shows that at almost every boundary crossing in the UK's energy supply chain, there is flow of money. Chang, Xu and Song's paper on the security risks of container shipping suggest that the payment between companies involved in a supply chain provides multiple significant security threats to the supply chain as a whole, including the exchange rate of currency changing during a payment which would increase the chance of delay, therefore compromising the availability of assets. A mitigation technique for the risks posed by payments could be to use a reliable third party payment company, such as *Stripe*.

ISO 27001, an information security management standard, suggests considering environmental-oriented threats alongside human-oriented and system-oriented threats [17]. In the UK, floods, heavy snow and storms are fairly frequent natural occurrences - taking precautionary measures for these threats, such as not storing goods in a building's basement in a flood-prone area, is advisable for companies involved in the UK's green energy supply chain.

5 Conclusion & Recommendations

The combination of more SMEs involving themselves in the UK's green energy supply chain (see Section 1.1) and SMEs being susceptible to security attacks (see Section 1.2) means that there is an increasing risk for all parties involved in the UK's energy supply chain, including the consumers.

Ideas and information created and tested by larger organisations who have greater security budgets is often a valuable resource for SMEs, who have a tighter budget overall. Examples of these resources include the National Cyber Security Centre's 12 principles of supply chain security, and large technology corporations' engineering sites, such as *Uber* (https://eng.uber.com/) and *Facebook* (https://engineering.fb.com/). NCSC's 12 principles are shown in Figure 2 and offer broad advice for all supply chains, while specific mitigation techniques, such as SSO and Principle of Lowest Priority can be adapted from analysing larger companies, such as *Facebook*.

Figure 2: NCSC's list of 12 supply chain security principles [18]

On top of looking externally for advice on security risks, I would recommend SMEs to complete internal risk analysis through the use of questionnaires, field studies and data analysis. Threats which have the highest risk should be given the highest priority and budget - those which have simple mitigation strategies should have those strategies employed, and those which are harder to mitigate should be covered by insurance.

SMEs who are not yet involved in the UK's renewable energy supply chain should invest large amounts of money into incorporating appropriate security measures into their business processes. Most attacks are human-oriented, however spending time and resources to develop a system's security can reduce the chance of human-oriented risks occurring without the need to remove employees from the situation.

Current-day developments on the UK's renewable energy supply chain will have to take COVID-19 into account, as it has caused major disruptions in supply chains around the world, particularly in the field of energy [19]. Future studies could explore this in more depth.

References

[1] "UK Government's website - UK becomes first major economy to pass net zero emissions law. Accessed: 25 Sept 2020." [Online]. Available: https://www.gov.uk/government/news/uk-becomes-first-major-economy-to-pass-net-zero-emissions-law

[2] "Carbon Brief - Analysis: UK low-carbon electricity generation stalls in 2019. Accessed: 25 Sept 2020." [Online]. Available: https://www.carbonbrief.org/analysis-uk-low-carbon-electricity-generation-stalls-in-2019

[3] International Energy Agency and the Centre for Climate Finance & Investment, "Energy Investing: Exploring Risk and Return in the Capital Markets," Imperial College Business School - Centre for Climate Finance & Investment, Tech. Rep., June 2020.

[4] "Sme definition - internal market, industry, entrepreneurship and smes." [Online]. Available: https://ec.europa.eu/growth/smes/sme-definition_en

[5] Ponemon Institute LLC, "2018 State of Cybersecurity in Small & Medium Size Businesses," Tech. Rep., November 2018.

[6] A. Yeboah-Ofori, S. Islam, and E. Yeboah-Boateng, "Cyber threat intelligence for improving cyber supply chain security," in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2019, pp. 28–33.

[7] "Supply chain security guidance - Website builders, NCSC. Accessed: 28 Sept 2020." [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security/website-builders

[8] "Supply chain security guidance - Third party software providers, NCSC. Accessed: 28 Sept 2020." [Online]. Available: ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers

[9] J. X. Chia-Hsun Chang and D.-P. Song, "An analysis of safety and security risks in container shipping operations: A case study of taiwan," *Safety Science*, vol. 63, pp. 168 – 178, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092575351300266X

[10] "Facebook protects users following Adobe hack attack, BBC News. Accessed 30 Sept 2020." [Online]. Available: https://www.bbc.co.uk/news/technology-24925874

[11] "Adobe confirms stolen passwords were encrypted, not hashed, CSO Security News. Accessed 30 Sept 2020." [Online]. Available: https://www.csoonline.com/article/2134124/adobe-confirms-stolen-passwords-were-encrypted-not-hashed.html

[12] "UK - National Grid Group. Accessed 29 Sept 2020." [Online]. Available: https://www.nationalgrid.com/uk/

[13] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th ed. Prentice Hall, ch. 1, pp. 9–20.

[14] "Protect your email by using a strong and separate password, NCSC. Accessed 30 Sept 2020." [Online]. Available: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

[15] "About the principle of least privilege, Indiana University. Accessed 30 Sept 2020." [Online]. Available: https://kb.iu.edu/d/amsv

[16] "The logistical challenges of wind turbine transport in the US, NS Energy. Accessed 30 Sept 2020." [Online]. Available: https://www.nsenergybusiness.com/features/wind-turbine-transport-us/

[17] "ISO/IEC 27001 — Information security management, ISO. Accessed 30 Sept 2020." [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[18] "Supply chain security guidance, NCSC. Accessed 25 Sept 2020." [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security

[19] "Renewables – Global Energy Review 2020 – Analysis, IEA. Accessed 25 Sept 2020." [Online]. Available: https://www.iea.org/reports/global-energy-review-2020/renewables