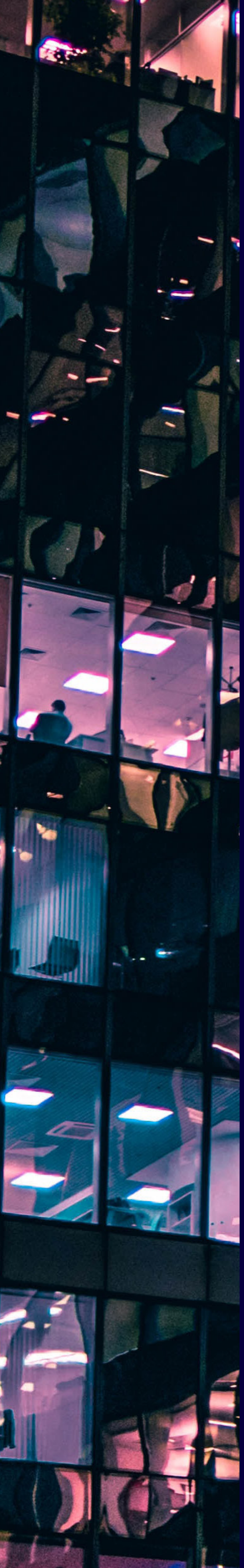
BEYOND
blue

PRAGMATIC RESILIENCE

by Alicia Waite, Associate Director



What is Operational Resilience?

Resilience has become the new corporate buzzword, but what does it really mean and how does an organisation become truly resilient?

Organisations are slowly accepting that focusing solely on preventative measures is not sufficient when faced with inevitable incidents and crises.

Many definitions of personal resilience highlight the need for self-awareness, adaptability and agility, but when defining organisational resilience, the focus is often on processes, structures and policies for incidents and crises. Such a theoretical approach risks stifling and even preventing people recognising and adapting to the incident or crises they face. Supporting good people in doing the right thing in a crisis is key to resilience.

This paper outlines a new approach to resilience using Beyond Blue's 8P model. This framework offers a new way for organisations to think about resilience in the increasingly dynamic and unpredictable world in which we live.

There is a difference between organisational and operational resilience. Operational resilience is one of three subcomponents of organisational resilience, alongside reputational and financial. These three areas are best understood by the type of crises they seek to mitigate:

- Reputational resilience: scandal or gross misconduct for example sexual harassment or child labour.
- Financial resilience: changes in demand, fraud or credit pressure.
- Operational resilience: factory fire, pandemic or cyber-attack.

These three areas are not mutually exclusive and often overlap. A severe cyber-attack, for example, can start as an operational issue but quickly have a material impact on a firm and reputational implications if the firm does not have a clear customer focussed communications strategy.

2020: A YEAR TO FORGET

Many people on the eve of 2020 were glad to see the back of 2019. Little did they know what 2020 would have in store.

Much of the world spent the year in and out of national and regional lockdowns with the UK implementing a seemingly everchanging tier system. As the world adapted to working from home, technology providers were hit with an unprecedented rise in demand and the likes of Zoom, MS Teams and Slack hit the headlines with security or performance issues as their userbases grew exponentially overnight. Whilst a Brexit trade deal was agreed at the close of 2020, existing supply chain issues have been, and are likely to continue to be exacerbated by inevitable teething issues in the implementation of the deal.

The world's largest economies have been decimated; the IMF predicted a 4.4% fall in global GDP in 2020 with the UK and the Euro area falling 9.8% and 8.3% respectively (IMF,2020). Whilst the IMF's 2021 projection is positive it won't restore countries to pre COVID-19 levels and organisations will be taking a prudent stance, conserving cash and reducing costs as they face huge uncertainty for the next 18-24 months.

With a backdrop of varied governmental COVID-19 responses, Brexit and the highly charged US election, geopolitical tensions continue to rise with accusations of foreign interference, disinformation campaigns and state sponsored cyberattacks.

In December 2020 the US accused Russia of a supply chain cyber-attack which led to the compromise of many US government networks. In Q3 2020, there was a 50% increase in the daily average of ransomware attacks, compared to the first half of the year (Check Point, 2020) and many threat actors are now extorting money from organisations not just to unlock encrypted systems and data, but also to preserve the confidentiality of their data. High-profile victims included Travelex, Garmin and Honda with some reportedly paying multi-million-pound ransoms.

In October, the US Treasury and G7 took a much harsher stance, threatening civil penalties against organisations who made or helped facilitate ransomware payments to cyber criminals on the US sanctions list (US Treasury, 2020). Organisations who fall victim to ransomware and in part, their cyber insurers, now face the unenviable dilemma of choosing between potentially astronomical manual recovery costs (if recovery is even possible), versus similarly large fines from governments.

COVID-19 was not 2020's only crisis. Time is running out for the world to act on climate change, Black Lives Matter protests have taken place in over 4000 cities, and the Wirecard scandal and US House antitrust report on the Big 4 Tech companies are the latest in a series of events which have increased widespread distrust and scepticism of big business. As a result, organisations find themselves being pulled in opposing directions by their stakeholders.

Customers and employees expect organisations to have a voice and play their part in social injustice and climate change. Investors are applying increasing pressure on the organisation's sustainability with ESG investing (Environmental, Social and Governance) soaring in popularity with ESG-themed exchange traded funds topping US$100bn in total assets for the first time in July 2020 (ETFGI, 2020).

Meanwhile, governments and regulators increase oversight and regulation, requiring growing overheads to sustain compliant operations, while organisations try to remain immune to a constantly changing geopolitical backdrop.

So how do organisations ready themselves for an increasingly dynamic and unpredictable future with a certain period of austerity?

The Regulatory Perspective

A key focus for financial regulators is the regulation of operational resilience. The key UK financial regulators released a discussion paper in 2018 on the topic which is expected to become Policy in 2021. Regulators around the world have since followed and released similar views in the form of formal consultation papers and guidance material. There are six core principles shaping the current view of best practice.

GOVERNANCE

The need for clear Board level accountability and senior management responsibility for resilience, informed by transparent and timely management information (MI) reporting. The Board and Senior Management must evidence how resilience considerations have shaped future investment decisions.

IMPACT TOLERANCES

Impact Tolerances are an organisation's tolerance for disruption to an IBS. It is the threshold at which that disruption caused intolerable harm to customers, to the organisation or the broader economy. This is not just a time-based metric and should include measures such as the volume of customers or payments impacted. An impact tolerance will likely exceed the traditional Business Continuity metrics of Recovery Time Objective or Recovery Point Objective. Impact tolerance is also separate to and will likely exceed risk appetite. Firms may need to identify impact tolerances for the firms, its customers and the industry, depending on the regulatory ring fences they fall into.

SCENARIO TESTING

Using several inputs including the organisation's cyber threat landscape, risk assessments and past incidents, identify scenarios capable of testing the impact tolerances for each IBS. Scenarios should look to simulate impacts on the availability & integrity of the resources that the organisation has mapped to each IBS, for example unavailability of people, failure of third parties, or a cyber-attack impacting technology & data.

IMPORTANT BUSINESS SERVICES (IBS)

Moving away from the traditional Business Continuity view of business processes and activities to important business services (IBS) that cut across traditional organisational silos and take a customer view of a service e.g. taking out a mortgage or insurance product. The focus should be on identifying the services that are truly critical to the organisations, its customers and the industry. Once identified organisations should map the resources (people, assets, technology, data and third parties) that support the service and therefore require prioritisation for resilience gap assessments and potential investment decisions.

OUTSOURCING AND THIRD PARTIES

In response to an increased use of cloud service providers and dependency on a small number of third parties, policy makers are keen to reinforce the message that organisations cannot outsource risk responsibility with the introduction of exit plans and substitutability for strategic or material third parties and outsourcers For all industries, COVID-19 saw lead times grow exponentially and highlighted the need to truly understand supply chain dependencies well beyond the obvious key third parties, drilling down into fourth party and high order dependencies to identify the weakest links. For organisations that have adopted just in time supply chain models, they will need to consider contingency measures to avoid the inevitable folding of suppliers, transport disruption and border restrictions in the immediate future.

COMMUNICATIONS

An organisation may be top of the class in their ability to respond to and recover from a crisis, but if stakeholders are not identified, prioritised and communicated to, this is a wasted effort. During incidents, media outlets and social media will fill the empty space left by absent corporate communications, with speculation and false information and organisations quickly lose control of the narrative. Drafting communications strategies, stakeholder mapping and agreeing communication channels are essential activities to aid efficient communication to help mitigate the impact on stakeholders and protect the organisation's reputation.

Beyond Blue believes there are 3 other key principles to consider when developing an effective operational resilience program.

Minimal Viable Company (MVC)

The MVC is core to all aspects of organisational resilience and should be defined before organisations identify and map their IBS. Key to defining the MVC is understanding what viable means to the organisation. For many, a key element will be a core set of profitable services or products. Therefore operations, reputation and finance need to be considered:

- **Operational:** The MVC is the operational core of an organisation which serves as the foundations for the IBS. This core is compromised of the foundational technology infrastructure, critical data, supply chain, associated skills and expertise, and assets that the majority, if not all, of the IBS are dependent upon.
- **Reputational:** Without customers and demand for an organisation's services or products the organisation loses competitive advantage, which over time will impact its bottom line. Organisations must both understand and consider their critical customers and the basis of their reputation when responding to incidents and crises.
- **Financial:** The ability to preserve the organisation's operations and reputation is dependent on having sufficient financial means. The MVC needs to both define and preserve an agreed minimum level of cash and assets, and appropriate balance of liquidity and capital to do this.

In any crisis, the preservation of the MVC will dictate the organisation's response and be critical in the event of a worst-case scenario or black swan event. The potential controls that might be used to protect an MVC (in line with the organisation's risk appetite) may be resource intensive, costly and complex to implement, so it is key that the MVC contains only those services and resources that are critical to survival.

RESILIENT CULTURE

Any concept, be it sustainability, innovation or inclusivity will only be truly achieved when it penetrates organisational culture and is embedded as a core value. Different approaches have varying levels of success which are heavily dependent on the existing organisational culture. Resilience can be closely aligned to a number of other operational concepts that organisations typically strive to embed, such as the importance of employees as the first line of defence against the cyber threat, and if done correctly can help organisations working to become more innovative and sustainable.

RESILIENCE BY DESIGN

A key tool in achieving a resilient culture is embedding resilience in the design, procurement and innovation of the organisation's products and services, specifically those involving technology and third parties. Many organisations attempt to conduct assessments of privacy or security at the end of these processes, undermining the importance of resilience. This means that only retrospective mitigating controls are available (if indeed they can be retrofitted at all), and the organisation loses the chance to take a forward look and build effective systems from the start.

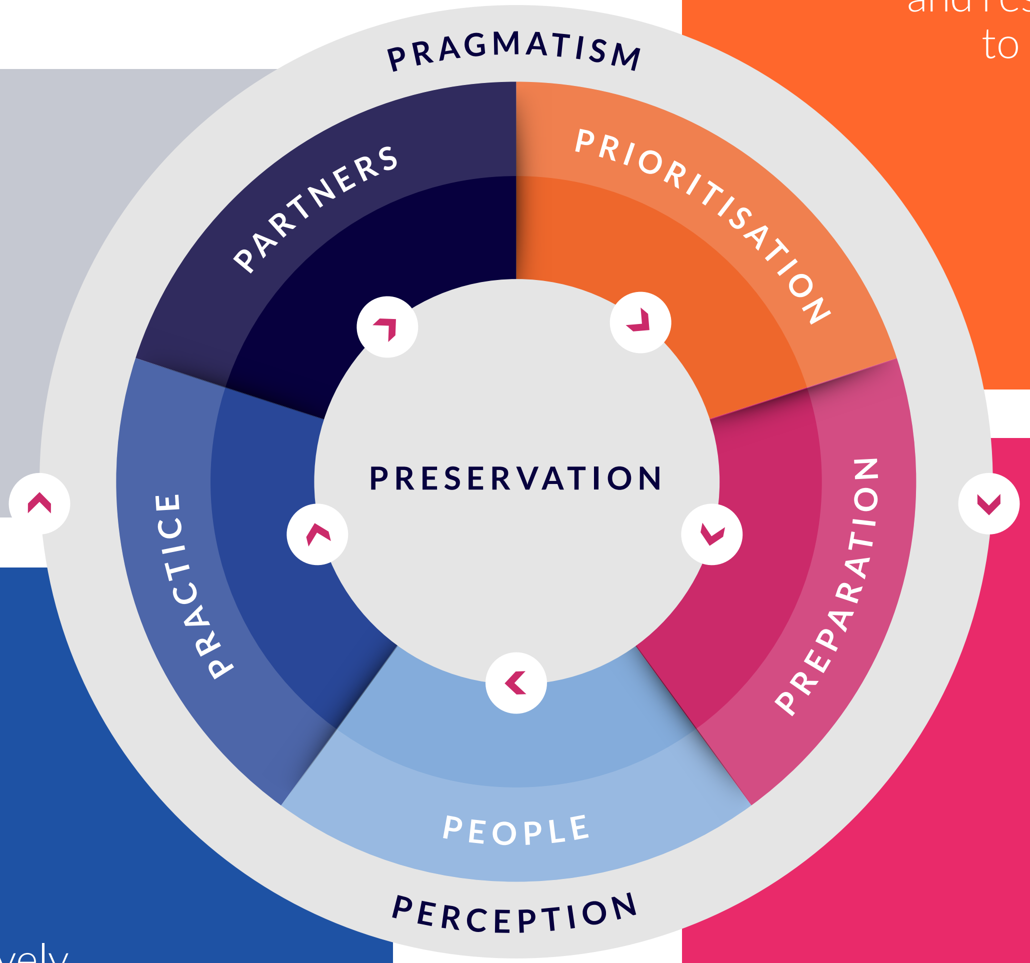
So how do you tailor these principles to your organisation and successfully implement them?

Eight Principles of Resilience – The 8Ps

Beyond Blue have developed an 8P framework for resilience. We can assist organisations with each of these areas but purposefully steer away from offering clients a list of services, recognising that there is no 'one size fits all' approach. Instead, the team listens to client problems and requirements and work together with them to identify how the team can provide the most value.

PRESERVATION

Central to the model is the concept of preservation. The definition, agreement and protection of the MVC should drive a resilience program's objectives. Understanding and preserving the lifeblood of your business will help focus investment in the right places, promote a pragmatic approach and inform the Executive's initial response strategy and actions during a crisis.



PRIORITISATION

Once the MVC has been agreed the organisation can define the IBSs that support it, followed by mapping the supporting activities, processes and resources (data, people, supply chain, technology and assets) to identify critical dependencies and resilience gaps. This will drive organisations to prioritise the most critical gaps and remediation activities and inform investment decisions in areas such as legacy infrastructure. Alongside the MVC, the understanding of the IBSs will drive an organisation's initial response strategy and be a key source of information when identifying impact.

PRACTICE

Practice highlights the importance of testing plans, assumptions and impact tolerances and training and exercising the people responsible for response, using severe but plausible scenarios. Many organisations carry out regular tabletop exercises and technical testing of disaster recovery plans, but these are typically isolated to individual teams or specific scenarios which do not effectively simulate the pressures and impacts of communicating and coordinating an effective organisation wide response.

Training and exercising are also key for the organisation's first line of defence; its staff, and even more so when cybercrime targets an organisation's remote working solutions. Naturally there is an increased attack surface as workers are geographically dispersed and utilising a wider range of technology, devices and tools to conduct their jobs.

PREPARATION

The success of operational resilience is dependent on appropriate governance structures. Organisations should define the role of the Board and Executive in their support, oversight and challenge of resilience activities and risk. Pragmatic and adaptable governance structures are also key to effective incident and crisis response with nominated decisions makers, escalation procedures and invocation criteria. These governance structures and the teams within them can benefit greatly from appropriate plans and risk -based, scenario specific playbooks which provide guidance, processes and procedures and considerations in different scenarios, if those responsible received adequate training in their use.

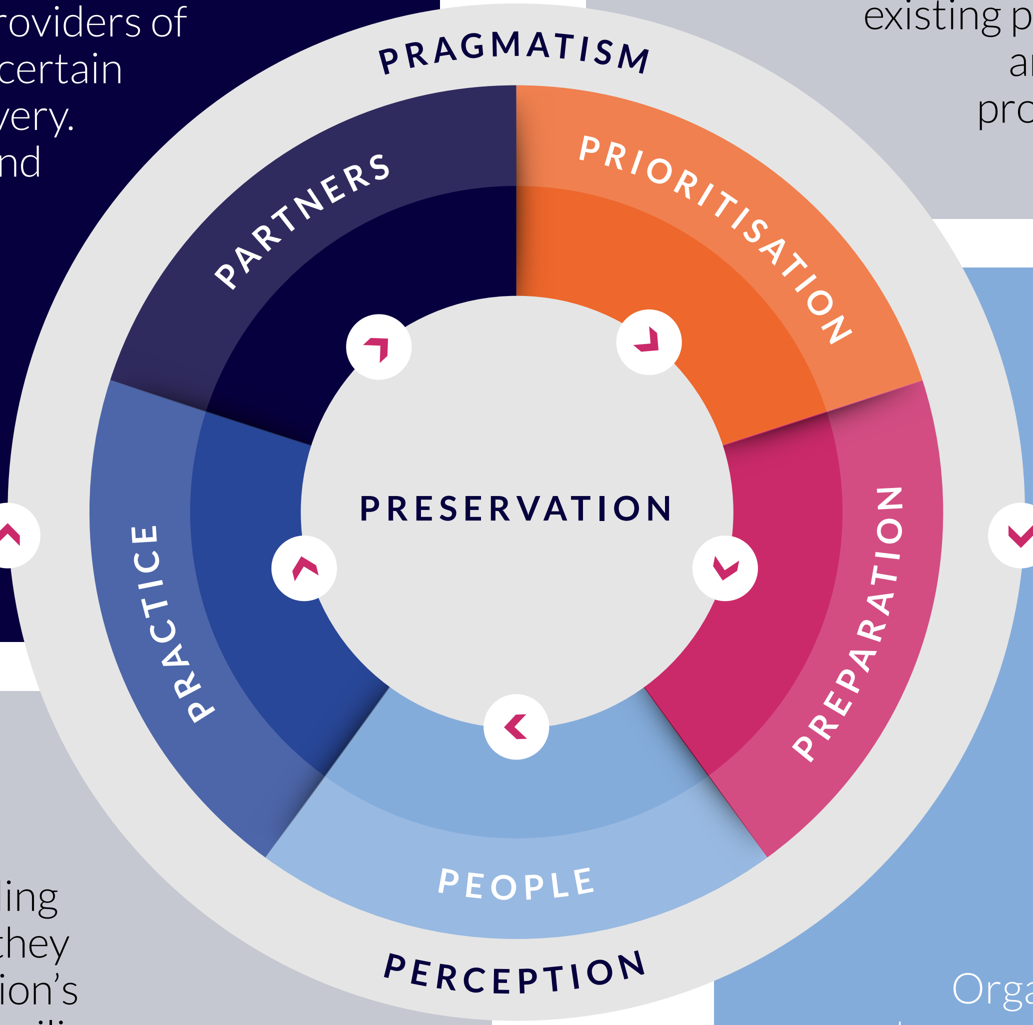
Eight Principles of Resilience – The 8Ps

PARTNERS

When it comes to resilience, partners can be both a help and a hinderance. In peace time it is key to understand the dependency that your IBS' have on supply chain partners and what assurance you can achieve of their resilience. For key suppliers, organisations must also identify their dependency on fourth and fifth parties, a notoriously difficult and subjective task. But third parties can also help organisation increase resilience as providers of substitutability and redundancy. Outside of supply chain, certain partners can be key allies during crisis response and recovery. In the event of a cyber-attack, resulting in a ransom demand and/or data breach, legal counsel, forensic investigators and communications firms are a key triad of support and advice for senior leadership, who often lack the knowledge to effectively and efficiently respond to such a scenario. Establishing this triad (or ensuring access through an insurer) before you need them, exercising with them and developing relationships will provide the foundations for an effective response.

PRAGMATISM

Whilst 2020 is perhaps the best-case study to support the need for operational resilience, recession and slashed budgets will demand that it is delivered in a pragmatic way. Resilience is key to an organisation in the (usually) infrequent event of operational disruption and to its long-term success, but it is important that the programme successfully evidences quick wins, leverages existing programmes or tooling, seeks automation (where possible) and delivers value. Doing so will always be a challenge for a programme that does not seek to directly boost revenue and therefore a risk based and MVC led approach is key.



PEOPLE

The start of this paper highlighted the need to not lose sight of the elements of personal resilience that are crucial to an effective and timely response and the reminder that it is people who enact the organisation's response, not just the carefully crafted processes, methodologies and tools. Teams and individuals responsible for operational resilience should be trained, empowered, and have processes and tools that are pragmatic and practical and provide space for personal resilience and judgement to prevail, albeit with a clear audit trail for decisions made and accountability accepted.

Organisations should seek to embed a resilient culture to help nurture employees' personal resilience, supported by awareness and training programmes. The approach for achieving this will differ for each organisation but typically requires senior, top-down support, the adoption of resilience as a business responsibility, incentivisation of employees and creating an organisation that is resilient-by-design.

PERCEPTION

Board and senior management's awareness of resilience is dependent upon the metrics and MI they receive. Effective metrics have to find a balance between overloading audiences with information and being too high-level that they do not inform decision making and status of the organisation's resilience. An organisation's stakeholder's perception of resilience is essential to its reputation. During a crisis, communications can make or break customers and the public's opinion of an organisation. Preparing robust communications playbooks with draft scenario specific communication strategies for employees, regulators, customers, suppliers and the media will be critical to reassuring stakeholders that an organisation is managing a crisis effectively.

Conclusion & Next Steps

The last year has highlighted the need for organisations to focus on their resiliency, regardless of whether it has been mandated through regulation. It has also provided a rare opportunity to learn from an operational disruption of such scale that senior leadership teams cannot ignore the findings and the need to be better prepared. Whilst buy-in may not be the issue, Boards and Executives will expect a programme that demonstrates value, effectively measures progress and translates into sustainable BAU processes and therefore a pragmatic approach is essential.

Things are looking up...
At the time of writing, several pharmaceuticals have developed, distributed and vaccinated millions of people at record breaking speed, providing a much-needed light at the end of the tunnel. In November last year the first commercial flight, Space X's Crew Dragon capsule named Resilience took 4 astronauts to the moon. Not even the sky is the limit when you get resilience right.

GET IN TOUCH

Please get in contact with a member of the Beyond Blue team to find out more about our 8P model and how we can help set up your organisation for success in an increasingly unpredictable environment.

David Ferbrache OBE
Managing Director
E: ferbrache@beyondblue.tech

Paul Taylor FREng
Director
E: paul.taylor@beyondblue.tech

Alicia Waite
Associate Director
E: alicia.waite@beyondblue.tech

BIBLIOGRAPHY

Check Point. (2020, October 6). Global Surges in Ransomware Attacks. Retrieved from Checkpoint.com: https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/

ETFGI. (2020, August 21). ETFGI reports assets invested in ESG ETFs and ETPs listed globally broke through the US$100 billion milestone at end of July 2020. Retrieved from ETFGI.com: https://etfgi.com/news/press-releases/2020/08/etfgi-reports-assets-invested-esg-etfs-and-etps-listed-globally-broke

International Monetary Fund. (2020, October 7). World Economic Outlook Update, June 2020. Retrieved from www.imf.org: https://www.imf.org/en/Publications/WEO/Issues/2020/09/30/world-economic-outlook-october-2020

New York Times. (2020, July 3). Black Lives Matter May Be the Largest Movement in U.S. History. Retrieved from nytimes.com: https://www.nytimes.com/interactive/2020/07/03/us/george-floyd-protests-crowd-size.html

U.S. Department of the Treasury OFAC. (2020, October 1). Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments. Retrieved from treasury.gov. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf