[Johns Hopkins COVID-19 Heat Map Tracking]

Threat Intel:

SARS-CoV-2 has been exponentially spreading within the global community and the effects of the virus and its attendant disease (COVID-19) are rapidly causing shocks within the global community. The affects of the pandemic are far reaching, we have seen the strain on the global supply chain as China fell into the height of the pandemic with supply chains being diminished or broken outright. As such, as the virus spreads, it is important to consider the threat space to the security and function of your organization due to loss of these supply chains as well as work forces within and without. As the spread of this disease continues, expect more supply chain degradation if not complete failures for some amount of time as the quarantines commence and play out.

As such, here are some basic questions to consider for your organizations security and continuity both as a whole and as separate functions such as the security of your networks. Use this document to spark discussions around the security response as well as the larger continuity and integrity of the whole as we are affected by this pandemic. These scenarios may not actually come to pass, but, as a security body, it is our job to forecast eventualities and the responses to them that might be needed to continue the function of the org.

Executive Briefing:

With the outbreak of SARS-CoV-2 and it's resultant COVID-19 (syndrome from infection) we have been seeing the arc of this outbreak becoming a global pandemic. With that in mind, it is advantageous to start planning for the effects from this pandemic on the businesses that you are responsible for. In this assessment, we will be taking a look primarily at the CIA Triad of the response but not just on a data security level, but, at an expanded outlook on the security, continuity, and supply chains that make

up the the CIA triad. All of these affect the security of your organizations as well as the basic functionality of your business.

With this in mind, it is important to look to the effects of the pandemic projecting out from initial outbreak to pandemic globally and how that will affect your business. Primarily the effects can be broken down into these discreet areas of concern:

1. **Supply chains:** What supply chains will be affected that will impact your business model?
    - ***Human capital, how many people does it take to function properly if the work force is down from COVID-19***
        - What are your tolerances on head count?
        - What contingencies do you have if work force is depleted due to sickness and quarantine?
        - Where are your single points of failure in the knowledge base were these assets to be sick and quarantined?
    - ***Supplies on demand that go into making your product; How much tolerance do you have for supply chains breaking?***
        - What regions do your supplies come from?
        - Are they affected now?
        - Plan for pandemic loss of work forces and how long you can function without supplies or with less

2.) **Infrastructure Capacities:** What tolerance does your network have to expanded remote working capabilities?

- ***With a workforce that may be in social isolation mode, what is the capacity for your company to allow people to work from home?***
    - People will self quarantine if they become ill
    - Children may be home as schools and day care shut down in order to prevent spread of disease
    - The state and federal government may recommend that people stay home and isolate to stop spread
    - In a protracted scenario of isolation and potential re-infection, what are your projections on your organizations ability to function?

3.) **Information Security Events and Response:** With a global pandemic, the same draw down on work forces will also apply to MSP's (SOC) workers as well

- ***With automation today much of the function of a SIEM/SOC is canned response, but, there is always a need for human intervention, who handles your response?***
    - During the time of pandemic and response, if your team is depleted due to sickness or quarantine procedures, what is your contingency for response?

- During the time of pandemic and response, the same applies to your SIEM/SOC solutions that you pay for if you do not have it in house, what is their contingency?
- If you have a true incident in your environment, how will you handle it if the primary incident handlers are unavailable?
- Do you have a service you work with?

All of these questions should be addressed going into an event like the one that is playing out globally with the SARS-CoV-2 (COVID-19) pandemic today. It is recommended that the executive suite be briefed on these questions and assure that these possible eventualities can be answered by the organization to insure the continuity of the org. Other elements of this narrative also come to bear on scenarios in others areas such as infrastructure, and overall output of whatever your organizations products are, but these are a good set of questions for the security element to bring to the executive suite to have the initial discussions.

As such, use this document accordingly.