The 2024 Elections and the potential for Business Disruptions

1. **Background and Risk Identification**

1.1. We are one year away from the election, and six months away from the start of election campaigns, rallies and other events.

1.2. There is a history of security incidents related to past elections in Indonesia and it is likely that campaign events will trigger security incidents that may cause business disruptions.

1.3. It is never too early to start preparedness and building resilience for business disruptions of any kind.

1.4. As in previous elections the authorities will likely identify high risk areas with the potential for unrest or conflict linked to:

- Electoral fraud
- Identity politics
- Negative campaigns - highlighting errors or shortcomings of candidates
- Black campaigns - untruths and fake news about candidates

1.5. Whilst we would all like to see a peaceful election process, the reality is, that there will likely be security incidents.

2. **What can we do in response?**

2.1. There are many ways that we can prepare and mitigate the risks related to the elections.

2.2. Here are our top four actions to support preparedness and build resilience related to the identified elections risks:

3. ACTION ONE - Monitor the Elections for Security Incidents

3.1. Establish an effective monitoring process that will bring you the latest reporting on security incidents related to the elections.

3.2. This process should capture reporting from the media, social media[1], and exploit all available professional networks to capture specific and credible reporting.

3.3. This process should cover areas where your staff live and operate, and all areas of business operations; sites, facilities, and supply chain routes.

3.4. This process should also provide staff with the latest updates, normally in two parts:

- ■ Part One - Reporting of security incidents - the facts and what is known
- ■ Part Two - Advisory action to take in response to the identified incident or related risks. This could include but not be limited to:
  - areas to avoid
  - behaviours to avoid
  - actions to take
  - advice linked to the Business Continuity Plan (BCP)

3.5. Providing this monitoring and information service will give your staff and business partners confidence in your levels of preparedness and mitigate the potential for disruption to normal business operations.

4. ACTION TWO - Business Continuity Plan (BCP) Health Check

4.1. The BCP provides the reference for all incident and crisis response, and recovery, but is rarely used or referenced at the time of incident.

4.2. It is therefore important that the core BCP activities are kept in-date and current.

[1] Social media will play an important role in the 2024 elections - see Action Four - Para 6.3

- Regular Threat Vulnerability & Risk Assessments (TVRA) have been conducted to support Business Preparedness and Resilience - The TVRA is the first step to clearly seeing your business and its associated threats, critical assets, security gaps & vulnerabilities, and operations to protect as well as the consequences for protecting and the risk-mitigation options that support lowering the overall cumulative risk.
- A separate TVRA should be conducted that uses likely Elections Incident Scenarios.
- Staff, assets, information, operations, supply chain, and ALL normal activities should be included in the BCP
- Roles and responsibilities within the BCP, have been identified - Training has been given to those with those roles and responsibilities.
- The BCP Crisis Communications Plan is regularly tested and all distribution lists are kept current.
- The BCP should be Realistic and Achievable.

5. **ACTION THREE - Emergency Response Services**

5.1. Even with an effective BCP, trained staff, business preparedness and resilience, incidents may still occur.

5.2. It is therefore prudent to ensure that an effective response team of trained security personnel would be ready to augment the existing security team to support and protect staff, assets, sites, facilities, and supply chain operations.

5.3. This is simply a Plan B, that would see the deployment of more security personnel.

5.4. If this was left until the time of need, it would be likely that all 'spare' local security resources would have already been contracted elsewhere.

6. **ACTION FOUR - Staff Awareness Briefings**

6.1. When actions 1-3 have been completed, it is then important to develop a staff briefing pack[2] on these elements, so all staff know and understand:

- What is in place
- What to expect
- The Communications Plan
    - How messages will be passed
    - How to report incidents or concerns
- Where to seek security support.

6.2. This communications rich strategy would be continued through the elections period via the monitoring and reporting process already detailed at action one.

6.3. Cyber Risk - The elections are likely to prompt increased cyber security risks and incidents. Consideration should be given to providing all staff cyber awareness briefings before the elections period.

7. Our assessment is that many elections related issues could trigger large security incidents under the collective heading of protest demonstration – the identified risk. We have therefore included in this guidance note our protest response guide.

7.1. **Protest Response a Four Point Guide**

7.2. Avoiding Risk

- Where possible simply avoid the protest risk and work from home.
    - The Protest Risk means;
        - Reported target protest locations

[2] It is a common failing that Hill & Associates find when working with client preparedness and resilience projects, that only the leadership team is well informed.

        - Main routes to and from those locations to transport hubs
        - Other potential secondary protest targets – i.e. other government sites in the vicinity
    - If it is not possible to work from home, then consider the following:

7.3. Communication

- Ensure your internal crisis communications systems/plans work – test them regularly
    - Time spent doing this will pay dividends at time of incident
    - If you are going to use WhatsApp or similar Social Media as your platform, then have clear user protocols.
    - Simply to group everyone onto one WhatsApp group and call it "*Our Crisis Communications*" does not work, may fail and expose staff to greater risk.
- Stay informed of what is happening through trusted sources.
    - The main media channels normally provide accurate information – sometimes live feeds from the incident location.
    - Trusted professional risk management partners
- Social media information is often incorrect – to counter this you should;
    - Communicate regularly to your staff.
    - This reporting should come in two parts;
        - Incident update – the known facts
        - Staff advisory response action – what they should and should not do

7.4. Physical Security

- Ensure your physical and procedural security is ready to lockdown in response to any protest related risks.
    - Test it and make sure locks and barriers work – maintenance is important
    - Make sure everyone understands the procedure for lockdown
- You may not be the target protest site but if you are close to a protest location or on a main route to a protest location you may attract risk by proximity.

4. Movement during Protests

- If there are protests in your area then do not move until an all clear has been given by the Police.
- Where possible get secondary confirmations from other trusted sources of this all clear reporting.
- Recent protests in Jakarta have been fast moving and the actual location of the protest risk has been fluid.
- Blocking the traffic at time of protest simply allows the protestors to move rapidly along empty roads.
- Get your drivers trained in the essential skills of route planning and defensive driving.

Golden Rule - Never move from a safe location to an unknown risk situation.

This guidance is not intended to replace regular all staff awareness briefings and internal emergency response and business continuity plans that are specific to operations, activities and the population at each location, but to provide a general quick reference pocket guide.

Never assume everyone knows what to do.

If you need assistance with your preparedness, resilience, BCP, staff training and briefing or any other element of your security risk management planning, then please do not hesitate to reach out to us for support.

PT Hill Konsultan Indonesia
Metropolitan Tower Building, 8th Floor
Jl. R A Kartini Kav. 14, Cilandak
Jakarta Selatan 12430
Indonesia
Tel: +62 21 5098 2050
Fax: +62 21 5098 2051
Mob: +62 811-1255-005 - Ibu Selly Oktavia