COVID-19 Impact: Crisis Management

Prof. dr. Sylvie C. Bleker-van Eyk
24 April 2020

pwc

Agenda

1. When does a situation become a crisis?
2. Leadership in crisis
3. Prepare, respond and recover
4. COVID-19 and fraud
5. COVID-19 and cybercrime
6. Communication
7. Never waste a good crisis
8. The aftermath of a crisis: emerge stronger through exit strategy scenario’s

When does a situation become a crisis?

Characteristics of a crisis

- **Sudden (natural disasters, disease)**
  - Mind! Often what is considered a crisis is a situation that has been lingering within the business and through triggering events it may become an existential crisis: e.g. when supervisory authorities pick up on the situation (corruption, sanctions)
- **Disruptive**
- **Affects important parts of your business: financial, human capital, reputation, operations, legal actions**
- **A perfect storm: COVID-19: never before was our world in (partial) lockdown affecting all everywhere**

Leadership in crisis

During a crisis, leadership must be prepared to go the extra mile

- **Abide by the three C's: stay cool, calm and collected**
- **Be brave: dare to make decisions!**
- **Stick to your values!**
- **Courage! Which also means the courage to prioritize**
- **Take responsibility: own the crisis and be a true leader and not a follower**
- **Collective thinking: you are not alone: your board, your employees and use their creativity, knowledge and experience**
- **Learn and analyze: primal reaction may adversely affect your exit out of the crisis**
- **Think about the different scenario's during the crisis and how they will affect the exit strategy**
- **Communicate as transparent as possible, but do not create panic by becoming overtransparant: Keep your eye on the crisis *and* the exit strategy**

Prepare, respond and recover

Prepare

You should be prepared for a crisis: crisis simulations must be part of yearly routine and company hygiene. Simulations on different issues: natural hazards, corruption, reputation, finance.

Be prepared and have teams ready to act with a protocol on key essentials

Respond

The preparation phase will give you one step ahead in the response phase. Leadership must be determined.

Think of the different scenario's and keep a survival exit strategy in mind!

Recover

Based on the exit strategy: emerge stronger, sooner and more resilient. During the crisis you must have held focus on the supply chain, financial position, employees and other stakeholders, so you can emerge stronger and fit for the future. Investigations may be necessary to recover funds, inventory etc.

COVID-19 and fraud

Fraud triangle: every action is based on *opportunity*, *pressure* and *rationalization*

Opportunity

- Given the fact that most people work remotely, and available staff is limited, normal effective controls might not be as effective as aimed for. Fraudsters know that and will try to make use of it.
- Regular checks and balances will not be as effective as designed. Accept and understand, business must continue, but use your common sense. In case of doubt, consult a colleague and take written note of your considerations.
- Usual requests for approval might be sent by others than known. Verify their identity by phone or in person.
- Currently there is a high risk on so called CEO-fraud (to be kept secret request by CEO to transfer funds). Always verify in person or by phone. Don't rely on email!
- Think as a fraudster. How would you from a fraudster view make use of the vulnerabilities organizations are currently facing? Close potential gaps or create a workaround.
- Be alert on new suppliers, change of addresses or bank-account-numbers etc.!

Pressure

- Suppliers (external) are facing difficult and uncertain times to come. Their future existence might be at risk. It is to be expected that business-partners might consider actions they would never ever had considered in normal circumstances. Realise this risk, discuss it with your business-partner and prepare yourself.
- Employees (internal) are facing the same uncertainties and fears as we all do. Take into consideration that employees used to be very loyal to your organisation, but now have to take responsibility for their own interest. Realise this and see how you would act from the current perspective in their position. Discuss this where possible and close potential gaps.
- National governments will announce, or already did announce supporting facilities (tax postponements, wages covering, compensation for losses etc). Organisations in severe conditions will try to make use of these facilities to the max. Not all organisations will be qualify for these facilities. They will try to get a kind of compensation on their own. Not always legitimate.

Rationalization

- People within our outside your organization will have the impression, sense, that current circumstances are not their fault. Others will have to be blamed for. So why should they take the burden of this crisis themselves? Realize what opportunities individuals might have to compensate their financial loss.
- No manager is happy to have to close down parts of his/hers organization. It is likely that managers will do everything to cook the books to avoid mass layoffs. Be prepared to evaluate figures and results from this perspective.
- If not happened already, it is not unlikely that nations, governments, leaders will blame other nations, governments and leaders for the massive outbreak of the current virus. The others will be considered as primary responsible, "the bad guys". It is not unlikely that (parts of) organizations will want to take 'revenge' for the current situation and will use this as a rationalization of committing fraud

COVID-19 and cybercrime

Cyber challenges faced

We are seeing both the likelihood and impact of cyber attacks increasing and cyber security good practices may fall by the wayside as organisations become more technology dependent than ever. We are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organizational change.

Our clients are facing the following challenges

- **A shift to remote working and prioritizing business operations brings an immediate risk increase**
- **Disruption to the workforce and suppliers will increase vulnerability to old risks**
- **Short staffing of security functions hinder effective detection of and response to cyber attacks**

We also expect that some cyber security risks are likely to be decreased as a result of changes. For example, a workforce operating from primarily home and travelling less will have a decreased physical security threat.

Key actions advised

Secure your newly implemented remote working practices.

Ensure the continuity of critical security functions.

Counter opportunistic threats that may be looking to take advantage of the situation.

Communication

Communication during a crisis

- **Stay cool, calm and collected: demonstrate your leadership**
- **Use the natural leaders within your organization: those are the ones that employees follow (leadership is NOT an ego-issue!)**
- **Communicate on the basis of facts and not emotions**
- **Deliver real, sustainable change that put their your employees at the heart of change.**
- **Communicate effectively in natural language**
- **Communicate on set times and only communicate in between the set times if its absolutely necessary**
- **Set up communication with your expert team (based on facts)**
- **Crisis communication is not per se usual communication as normally done by communication department: use external crisis communication experts**

Never waste a good crisis

Crisis opens the doors towards creativity

Working remote from home has its pitfalls but also increases creativity but beware of cybersecurity

At the university we normally give lectures. Now online, but a great idea is to keep recording lectures after lockdown and only use the lecture time for purely interactivities

Dealing with the COVID-19 crisis gives non-prepared organization a crash course in crisis management. Important to organizations is to respond adequately and the the lessons learned from this crisis to assure future crisis resilience

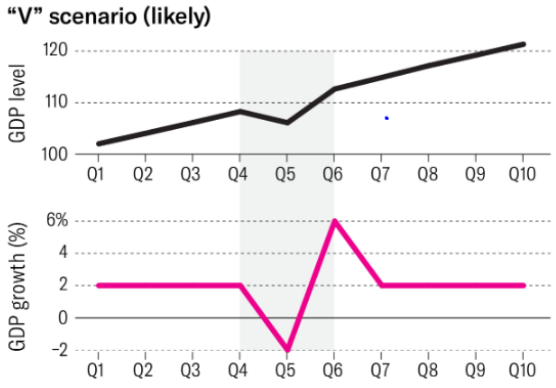
The aftermath of a crisis: emerge stronger through exit strategy scenario's

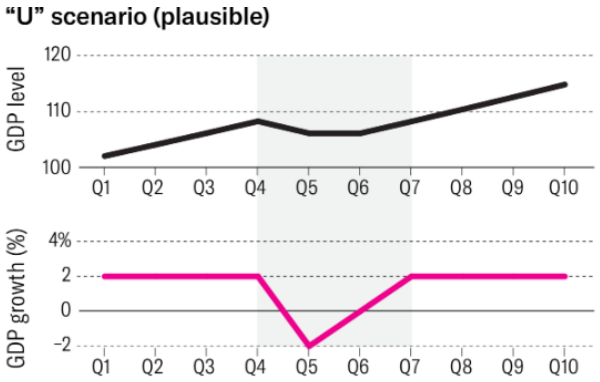
Aftermath COVID-19: think through the scenario's

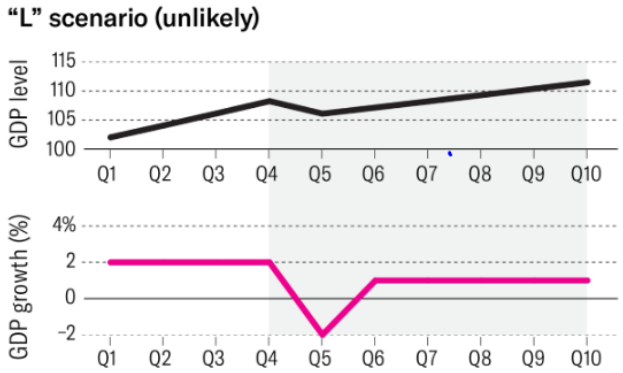
At a certain time in space the lockdown will finish. How can your organization reemerge from this crisis.

It is important to already think about how your organization will exit this crisis and fire-up business again. B2C and B2B exists by means of the customers, suppliers etc. The question is not only how you will emerge but also how others will emerge and enter into business with you

Harvard Business Review gave the following three main scenario's you should take into account;







Thank you

Prof. dr. Sylvie C. Bleker-van Eyk
Compliance & Integrity Management
PwC | Senior Director Forensic Services
Tel: +31 (0)6 83 80 20 37
E-mail: sylvie.bleker@pwc.com
PricewaterhouseCoopers Advisory N.V.
Thomas R. Malthusstraat 5 | 1066 JR | Postbus 9616 | 1006 GC | Amsterdam
www.pwc.nl

pwc.nl