

market leaders in
digital transformation

Supply Chain Management

How deep is “Deep enough”?





Table of contents

Supply Chain and Cyber Security

1. Supply Chain and Vendor Management	3
2. Contractual Clauses – Theory and Reality	6
3. Cross-dependencies on Major Disruptive Events	8

Supply Chain and Cyber Security Management

Supply Chain and Vendor Management

- On a Cyber-presence reality, resilience is the key
 - What is my business?
 - What are my Key resources?
 - What are my current client agreements and commitments?

Am I fully aware of my reality? ...from a 360° perspective?

Supply Chain and Cyber Security Management

Supply Chain and Vendor Management

- In order to keep a minimum set of services/products running and available,
 - Am I identifying every dependency?
 - Logical, Physical, Data,.... (how soon or quick will we be needing those?)
 - Prioritize according to your agreed Recovery Time Objectives
 - Are there anything that can wait or be deterred?
 - If I am relying on an external service (e.g: a SOC, a NOC)
 - Are those guys aligned with my priorities?
 - Are there any contingency scenario created and formalized?

Prioritize but do not leave relevant or critical assets out

Supply Chain and Cyber Security Management

Supply Chain and Vendor Management

- Regarding Services:
 - Is my SOC/NOC/Cloud/Datacenter resilient?
 - What about power supply?
 - What about Datacenter Cooling ?
 - What about maintenance, Are all my machines up-to-date? Patched? Maintained?
 - If a disruption occurs, how soon is my vendor able to replace my assets?
 - And whenever a major contingency, is it capable of maintaining that service?

Do we have all our dependencies covered?

Supply Chain and Cyber Security Management

Contractual Clauses – Theory and Reality

- Theory:
 - *“By Contracting a Service, my provider will provide it..”*
 - Contracts usually cover “normal circumstances” and a fail-proof clause (usually named as “Act of God”... 😊)
- Reality
 - In case a major disruptive event occurs, both you and your provider may be impacted
 - Contracts are commonly lacking
 - “Contingency Scenarios” and
 - “Minimal acceptable contingency levels of service”, together with realistic compensating amounts
(Are you (the business) willing to pay extra for them?)

Setup your priorities and create a fail-proof chain-of-trust

Supply Chain and Cyber Security Management

Contractual Clauses – Theory and Reality

According to your business, please do consider also as a Vendor or Supplier

- Water supplier
- Power Supplier, *(or a backup generator with a contracted fuel provider)*
- AC supplier with a stock of agreed replacement parts
- Accommodation *(If you have a contingency scenario that needs personnel relocation)*
- Contingency money or financial resources *(specially if there are relocated persons)*
- Alternative office site providers

Are all critical business needs covered ?

Supply Chain and Cyber Security Management

Cross-dependencies on Major Disruptive Events

- Third-Party contracts shall always include agreed Service Level Agreements, right?
 - What if....
 - Are my suppliers also impacted by the same incident? (which ones?)
 - Do I have an agreed “contingency scenario” with my provider, establishing both a contingency scenario and a minimum agreed level of contingency service?
 - I am relying on someone (e.g: External developer) that may not be available?
 - Do I have the source-code?

Take the challenge up to the Risk management / Risk Acceptance level

Supply Chain and Cyber Security Management

Cross-dependencies on Major Disruptive Events

- Cloud Solution Providers
 - Am I putting all my eggs into the same bucket?
 - Do I periodically test my resilience?
 - Am I resilient?
- About my Cyber infrastructure
 - Are all my relevant event records available or prioritized for recovery?
 - What will provide me more visibility, more accurately and quicker?
 - Are there independent sources of info I can rely to provide me a side-view?
- My SOC is provided by a third-party
 - Do we have contingency scenarios covering the human factor?
 - Do we have an alternative site?
 - Are the needed information resources available there?

Do not leave neither the Concerns nor the control of variables solely on the hands of third-parties

Supply Chain and Cyber Security Management

Be sharp, accurate and start small

- Setup your Core
- Prioritize
- Setup (and maintain) contingency scenarios for:
 - Physical location unavailability
 - Technological unavailability
 - Key-roles unavailability
- Perform regular testing for:
 - Checking completeness of your vendor list and critical vendors enumeration
 - Identify possible gaps in the program
 - Listen to your environment

The more critical your business is, the more thorough you have to dive...

Questions ?