

The Marriage of Digital & Operational Risk : The Search for Happy Ever After

Letitia Adu-Ampoma

Director
Peverett Maxwell

Presented at The Risk Summit Africa, Accra, Ghana
Wednesday, 22nd May 2019

A Journey.....

Honeymoons

Romance

Digital Risk

Operational
Risk



Awakening
of Joy

Stability

Power
Struggles

Disillusionment

Clarity & Sunsets

Storms

Some Definitions...

•Operational Risk

- The prospect of loss resulting from inadequate or failed procedures, systems, policies, personnel or external events
- The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Examples : Fraud (Internal/external), Employment practices & workplace safety, clients, products and business practices, Damage to physical assets, Business disruption and system failures, Execution delivery & process management

•Digital Risk

- Risk associated with digital business processes.

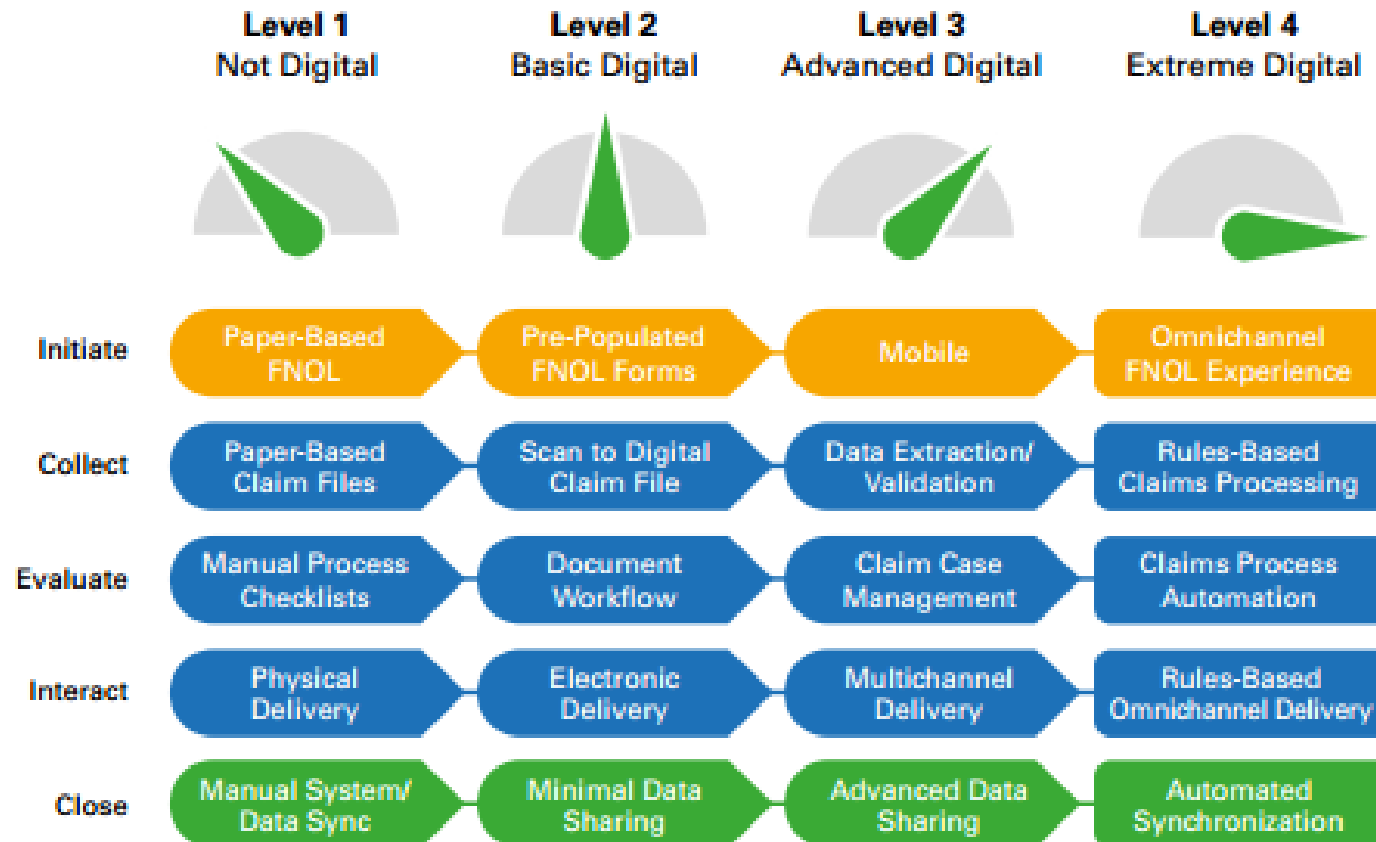
What is a digital business process ?

We need to understand the following...

Digitization	Digitalisation	Digital Transformation
<ol style="list-style-type: none"> 1. Taking analog information and encoding it into zeros and ones so that computers can store, process and transmit such information. E.g. converting handwritten or typewritten text into digital form. <i>(Source : Jason Bloomberg, Intellyx)</i> 2. Digitisation – the process of changing from analog to digital form. <i>(Source : Gartner IT Glossary)</i> 	<ol style="list-style-type: none"> 1. The use of digital technology to change a business model and provide new revenue and value-producing opportunities. It is the process of moving to a digital business. <i>(Source : Gartner IT Glossary)</i> 2. Digitalisation is the process of employing digital technologies and information to transform business operations <i>(Source : Gartner Inc)</i> 3. Digitalisation is the way in which many domains of social life are restructured around digital communication and media infrastructures. <i>(Source : Brennan & Kreiss, School of Media & Journalism, University of N Carolina)</i> 	<ol style="list-style-type: none"> 1. Customer – driven strategic business transformation that requires cross-cutting organisational change as well as the implementation of digital technologies. Digital transformation will typically include several digitalisation projects <i>(Source : Jason Bloomberg, Intellyx)</i> 2. Digital business transformation is the process of exploiting digital technologies and supporting capabilities to create a robust new digital business model. <i>(Source : Gartner IT Glossary)</i>
<p><u>Focus</u> Information</p>	<p><u>Focus</u> Processes, Roles, People interactions</p>	<p><u>Focus</u> Business & Strategy</p>



Basic Insurance Claims Example...







Source :
<https://www.experfy.com/blog/how-does-your-insurance-organisation-measure-up-digitally>

What is the relevance of Marriage?



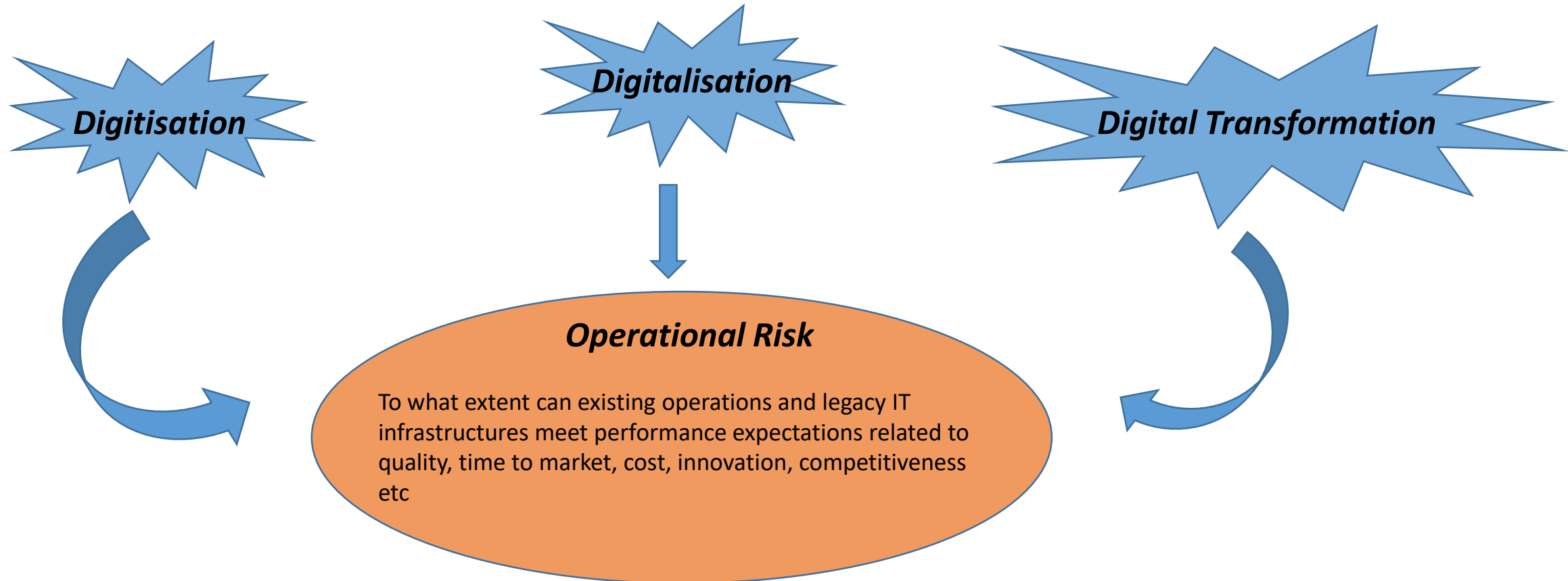
Digital Risk & Operational Risk – The Marriage !

External Digital Risks		Implications for Operational risk
Cyber-Attacks/Threats Data Leakage/Information Security The Dark Web Reputation Risks		Social Engineering /People People (Actions, Rights, Privacy, Governance) People & Process
Internal Digital Risks		
Process Automation Decision Automation		Impact on systems, processes and people , which are the core elements of Operational risk. Appropriately managing the digital risk associated with process or decision automation requires managing the operational risk.
Data Related Digital Risks		
Information Security Analytics, Advanced Analytics, AI Fake or True? Ownership/Responsibility Confusion		People Process Technology
Digital Technologies (which cause digital risk)		
Cloud, Mobile, Social Media, Big Data, 3 rd Party Technology Used, Internet of Things (IoT), Block Chain, Advanced Analytics		Implementation/Use of these technologies all impact legacy operations, processes and the availability/use of data and data flows.

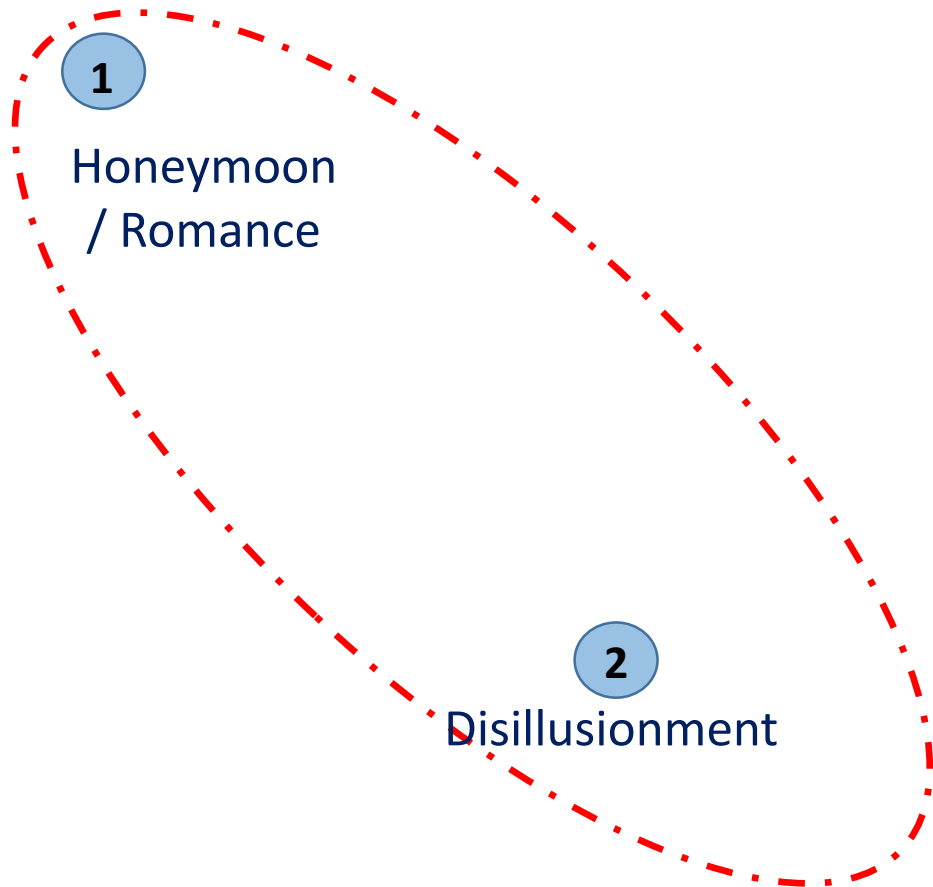
Digital Risk & Operational Risk

In addition remember....

A digital risk is a risk associated with a digital process



The journey to forever....



3
Power
Struggle

4
Stability

5
Awakening to
Joy

Examples of the Honeymoon Phase & The Disillusionment Phase

Honeymoon / Romance Phase

International Examples

Initial launches of innovative and disruptive new business with new business models

E.g. Uber, AirBnB

Rapid early growth of companies behind digital technologies like social media i.e. Facebook, Twitter

Local Examples

Online Banking launches

Mobile Money, Mobile Insurance & other Fintech
mHealth

Churches – Launches of ‘Digital Business’ e.g.
Presbyterian Church Ghana

Disillusionment Phase

International Examples

Aadhar – Indian Government Portal – 1.1 billion users
data breach (Discovered March 2018)

Facebook – Cambridge Analytica Scandal – 87 million
(Occurred 2015 and revealed 2018)

Google Plus – 52.5million (March & Nov 2018)

Local Examples

Some government initiatives e.g. Ghana Post App
– Digital Address

What Changed?

- Social Engineering

- The use of deception to manipulate individuals into divulging confidential information or personal information that may be used for fraudulent purposes
- Has increased in prevalence and sophistication
- Strategies used are deeply contextual and culturally specific

- 3rd Parties (Proliferation of)

- 3rd Party network complexity in the digital ecosystem (e.g. Facebook, Cambridge Analytica Scandal)

- Cloud Computing/centralisation

- All eggs are in one basket. An uncomfortable choice for operational risk

- Ethics, People, Privacy, Information & Data concerns

- Security and protection for the individual
- Transparency of digital solutions

Some Social Engineering Strategies

Social Engineering is in essence a form of cyber-attack which uses tactics to skirt all possible technical tools and solutions and instead exploit the weakness of human psychology. Social engineers use a variety of media including phone calls and social media to trick people into offering them access to sensitive information.

The key types of social engineering are as follows:-

- Phishing

- Most common type. Usually seek to obtain personal information via email.
- Use links that redirect users to suspicious websites in URLs that appear legitimate
- Incorporate threats, fear and a sense of urgency
- Attackers often pair malware with phishing attacks to steal users information

- Pretexting

- Attackers focus on creating a good pretext or a fabricated scenario to use to steal victims information

Some Social Engineering Strategies cont'd

- Baiting

- Similar to phishing attack but promises an item or good that hackers use to entice victims e.g. free music downloads in return for login credentials to a certain site

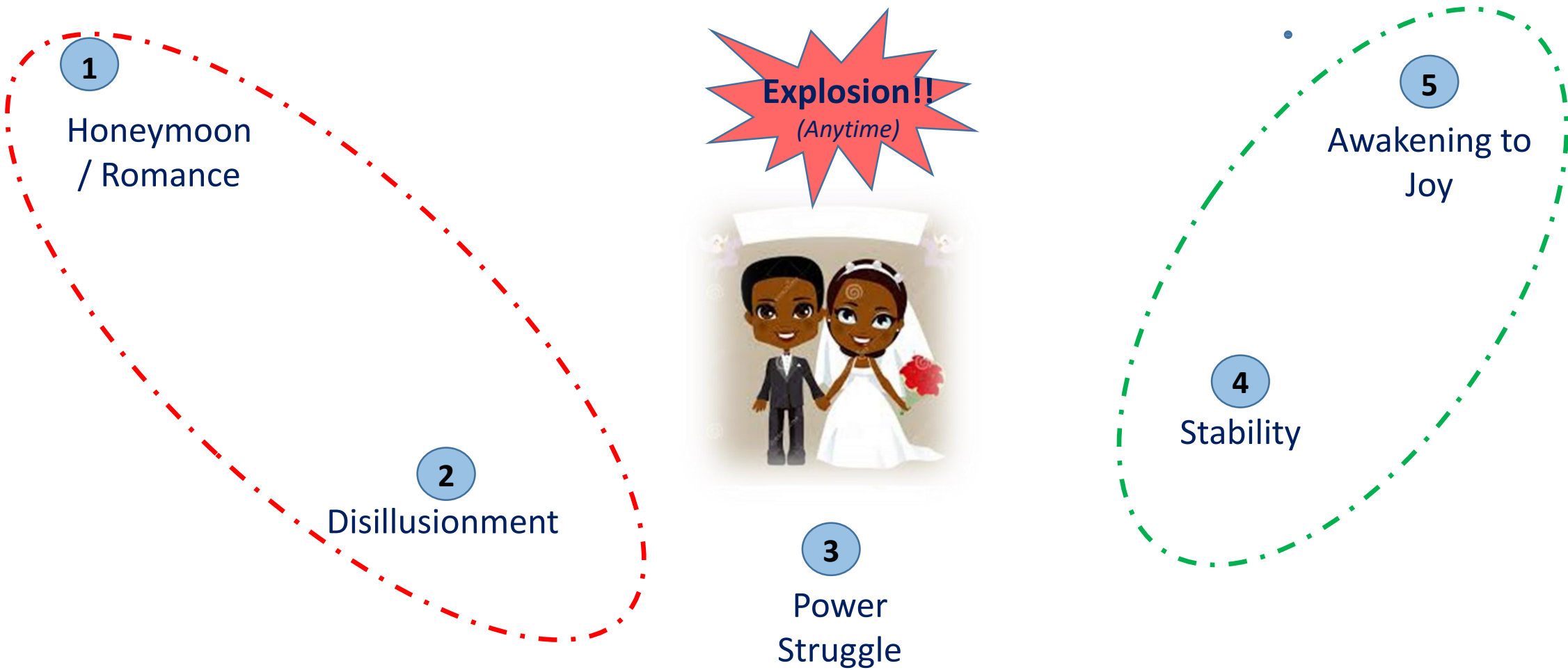
- Quid Pro Quo

- Promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.
- Common example : Fraudsters who impersonate IT service people and spam call as many direct numbers that belong to a company as they can find. The attackers offer IT assistance and a quick fix to a problem in return for the employee disabling their AV program and for installing malware under the guise of software updates.

Tailgating / Piggybacking

- Someone who lacks the proper authentication following an employee into a restricted area
- Common example : A person impersonates a delivery driver and waits outside a building. When an employee gains security approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access from someone who is authorised to enter the company

How do we get to the Happy Ever After?



A strategy to achieve the Happy Ever After

Governance + Culture + **Digitalised** Risk Management
=
Digital Risk Compliance Management



Governance



Provides the glue/frameworks which enable the habits, attitudes, beliefs and values etc that will help transition to the Happy Ever After

- The Governance must be ‘operational governance’, *not just* Boardroom Level governance, eg
 - Corporate Governance translated into basic procedures and actions for employees at all levels of the organisation. The corporate governance should take into account the digital strategy of the organisation and the procedure for managing digital risks.
(Remember : Digital risk is more than cyber – security risk!)
 - IT Governance (with supporting policies and procedures) AND procedures actually implemented and being followed
 - Information Security governance which should include the necessary supporting Privacy, Security and Data Protection elements.

Benefits

Will bring the FULL scope of digital risk to the attention of the business and make it a C-Suite item

Culture



A specific desired organisational culture does not ‘just happen’. It takes deliberate, consistent effort over time, with regular monitoring, measurement and corrective actions along the way.

But culture is/will be critical to having an effective ‘defence capability ‘ against social engineering – especially in a local context

- *Work* that needs to be done in relation to culture includes
 - Outline, agreement, vision and design of the desired culture
 - Clear agreed principles that underpin the culture – including ethics and approach to machine learning, robotic process automation, natural language processing, artificial intelligence etc
 - Training and education required (based on a specific needs assessment completed)
 - Clear framework of incentives, rewards and sanctions which the organisation needs to implement to shift the culture to the desired state
 - Supporting processes to shift behaviours, attitudes and operations to the desired culture
 - Identified people, change agents and leaders who ‘are of’ the culture desired
 - Change management framework for implementation
 - Continued monitoring and measurement.

Digitalised Risk Management



The most powerful way to effect and achieve a change one wants, is to change oneself!

Digitalisation and/or digital transformation is now a basic reality of business. Risk management as a function needs to embrace this and move with the digitalisation wave. This will enable 'Integrated Risk Management.'

• *This involves embracing some of the following based*

- Completing full assessments of digital readiness
- Competing digital risk assessments specific to organisations or specific business lines of an organisation
- Embracing digitalisation as a solution to effective management of digital risk eg scoping digital technologies to make the risk function more effective in digital risk management. Examples include:-
 - Advanced analytics
 - Machine learning tools
 - Process automation
 - Decision automation
 - Digitized monitoring and early warning



THANK YOU!

info@peverett-maxwell.com
www.peverett-maxwell.com