# CYBER AND DATA SECURITY RISK MANAGEMENT WORKSHOP

**Now Available as**
**In-House Workshop**

FOR BOOKINGS
CALL 0812 031 8671 | 0809 555 0641
EMAIL TO INFO@CONRADCLARK.COM


*If you don't like something, change it. If you can't change it, change your attitude. Don't complain. - Maya Angelou*

*…..inspiring ~~im~~possibility*

# Joachim Adenusi (Oga Risk)

- *Actuarial Science : BSc & PGD, Masters in Enterprise Risk Management: MSc*
- *Doctorate Programme – Risk, Crisis and Leadership (UK)*
- *Chartered Fellow & Former Director: Institute of Risk Management (IRM) UK*
- *Specialty: Enterprise Risk, Reward, Strategy & Performance Management*
- *Professional Awards: The UK Risk Manager of the Year 2009/10; EU Strategic Risk Awards 2007 & 08*
- *Visiting Professor & Certified Risk trainer - IRM & Chartered Insurance Institute (CII) UK*
- *Chief Risk Officer (CRO) - Public, Private , Financial Services, Health Sector & Oil and Gas*
- *Established the Nigerian Risk Awards…celebrating efforts in good governance*
- *Business Founder, Missionary and an imperfect man loved by perfect God*
- *One of the first 10 Certified Follows of the Institute of Risk Management UK – July 2015*

## CCN Malta Associate

### Patrick Mifsud

A senior associate in Conrad Clark Nigeria who comes from the sunny Mediterranean Island of Malta. He is an IT engineer by profession and comes from a systems engineering background.

Patrick joined SHIELD Consultants in 2010 as an Information Security consultant where he still works with clients to manage their information security risks and also assists them in their business resilience.He is also the General Manager of the company and together with his colleagues, they strive to keep SHIELD as the leading Operational Risk Management company on the Island.

Patrick has a BSc degree in IT and a MSc degree in Information Security from the University of London.

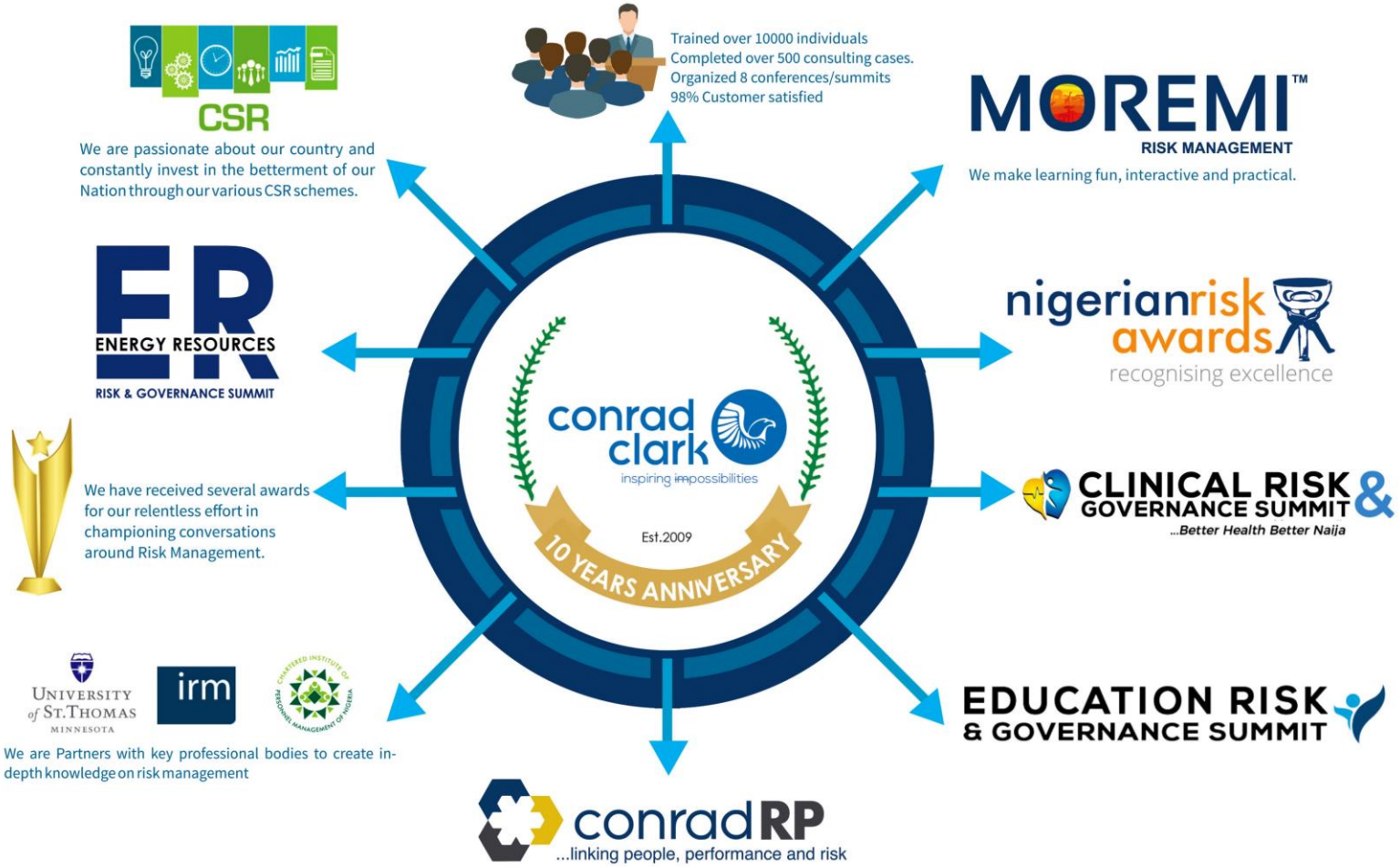
### Emma Cundiff

**FIRM MIoD (UK)**

**Emma** has over 20 years experience working in risk management consulting and training. Her clients come from a range of industries including manufacturing, travel and transport, biotechnology, healthcare, and education. She is a former Director of the Institute of Risk Management (IRM) serving on the board for six years. Emma is a Fellow of the IRM, a member of the UK's Institute of Directors.

Emma's driving principle is that if risk management is to be of any value in an organisation then it should be proportional to the level of risk.

# CONRAD CLARK @ 10




*"we exist to assure performance outcomes in an environment of uncertainties"*

# Our Objective ?

**Protection, survival  and growth of businesses (Org.) during and after COVID 19**

# ENTERPRISE RISK MANAGEMENT

## -ERM ADVANCED

(Virtual Workshop)

**Fee: #60,000**

**Duration: 3days**

**Time: 8am -12pm Daily**

FOR BOOKINGS

CALL 0812 031 8671 | 0809 555 0641

EMAIL TO INFO@CONRADCLARK.COM

# Data Protection

An Introduction

# Aims of the Session

- To understand
  - The meaning of data protection
  - The lawful basis for processing and handling data
  - The six principles of GDPR
  - How data can be lost

# Top Five Data Breaches of 2019

- Capital One (US)
  - Credit card application
  - Bank information and social security numbers
- Elastic search (108 million)
  - Online casino group
- Exactis – 340 million
  - Information on clients on a database which was publicly available
- Mongo DB
  - Database containing millions of records of Chinese job hunters
- US Government – Technology site
  - Hit by Malware - Emolet

# Definitions

- Data Protection
  - The process of safeguarding important information from corruption, compromise or loss.
- Handling Information
  - The process by which personal information is used, transported and stored.
- Confidentiality
  - The state of keeping or being kept secret or private personal information.

# Data Protection Regulation

- EU Data Protection Directive 1995
  - UK Data  Protection Act 1998 replacing the Data Protection Act of 1984.
- Data Protection Act 1998
  - To make new provisions for the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.
- Gave individuals the rights to control information about themselves.
- Compelled anyone holding personal data to comply with the act.

# General Data Protection Regulation 2018

- EU Data Protection Directive in place for 20 years
  - Minimum standards of data protection.
- EU decided on a single unified law – Two key goals
  - Protecting the rights, privacy and freedoms of EU residents.
  - Reducing barriers to business by facilitating the free movement of data.
- The regulation to be applied consistently throughout the EU

# Impact on EU states

- Cannot not be overturned/modified by a member state.
- Provides legal rights to ensure that data subjects are protected from the mishandling of their personal data.
- Regulations appears to be disruptive
  - Every organisation has to comply if they want to do business in the EU.
- Threat of punitive and dissuasive fines.

# Nigeria Data Protection Regulation 2019

- The key objectives of the Data Protection Regulation include:
  - safeguard of the rights of natural persons to data privacy;
  - foster safe conduct of transactions involving the exchange of personal data;
  - prevent manipulation of personal data and
  - ensure that Nigerian businesses remain competitive in international trade, through a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices.

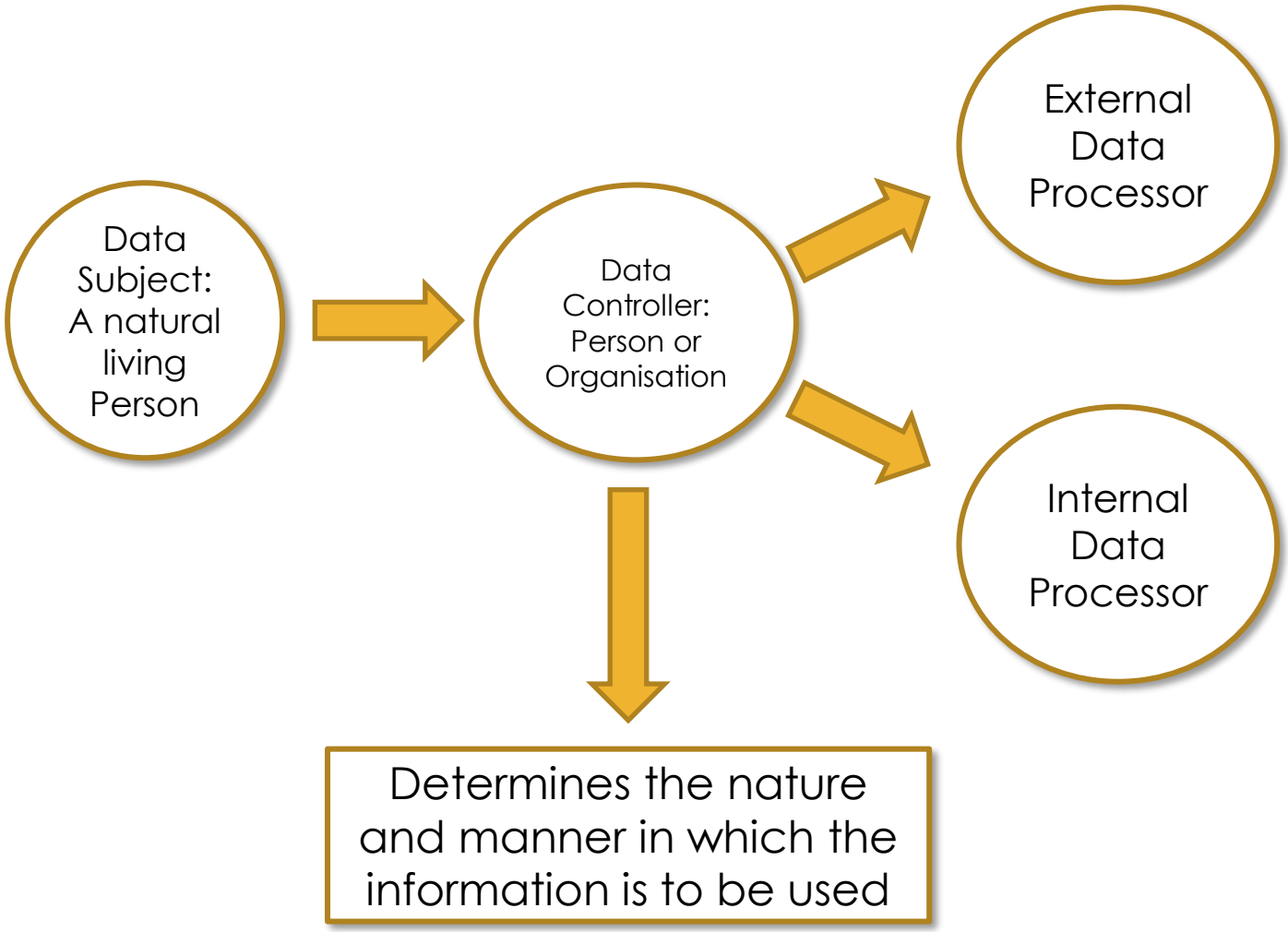
# Scope of the GDPR

- Applies to the processing of personal data wholly or partly by automated means.
- The processing other than by automated means of personal data which forms part of a filing system.
- Filing;
  - Personal data that is organised for easy access or use e.g.
    - Papers in a filing cabinet
    - Electronic database
- Exemptions – National Security

# Territorial Scope

- Organisations in the EU that process personal data even of the actual processing activity is conducted outside the EU.
- Organisations outside the EU that process the personal data of EU residents as part of offering goods/services or behaviour into the EU.
- Organisations outside of the EU that are otherwise governed by EU laws on the basis of public international law.

# Key Definitions



# Key Definitions

- Processing
  - Anything you can do with information from collection to destruction.
- Data Processor
  - Bodies contracted by the Data controller to perform some kind of function on the personal data.
  - Data controllers can be processors.
  - Written terms are obligatory.
- Sub-processor
  - Work contracted by the data processor to another party. Data processor must ensure that data is looked after.

# Personal Data

| | |
|---|---|
| **Name**<br>**Date of birth**<br>**Marital status**<br>**Phone number**<br>**Email address**<br>**Residential address** | **Salary**<br>**Education**<br>**Car registration**<br>**Tax information**<br>**Photographs**<br>**Bank account number**<br>**Driving licence number** |
| Hair colour<br>Eye Colour<br>Weight<br>Height<br>Defining characteristics<br>Number of days sick | IP Address<br>Browser Cookies<br>Geo-tracking |

This list is not exhaustive.
Any data that can identify an individual whether directly or indirectly is in the scope of personal data.

# Sensitive Data

| | |
|---|---|
| **Ethnic or racial origin**<br>**Bio-metric data**<br>**Medical information**<br>**Sex life**<br>**Sexual orientation**<br>**Genetic information** | **Political opinion**<br>**Religious beliefs**<br>**Philosophical beliefs**<br>**Trade union membership** |

Processing of this type of data is prohibited unless certain conditions are met;
Consent of the individual
Processing is required to meet certain obligations

# Six principles of GDPR

1) Fair, lawful and transparent

2) Data minimisation

3) Storage Limitations

4) Limited purpose

5) Accuracy

6) Integrity and confidentiality

# 1) Fair, lawful and transparent

- Fairness
  - The data controller is open and honest about who they are.
  - Obtains the data from someone who is legally authorised to provide it.
  - Handles the data in ways that the data subject would expect.
  - Does not use the data in ways that might unjustly have a negative effect on the data subject.

# Transparent

- Data controller to tell people clearly and openly how they intend to use their data (unless it is obvious).

# Lawful basis for processing (1)

| Consent | The individual has given clear consent for their information to be processed for a specific purpose. |
| --- | --- |
| Contract | The processing of the information is necessary for a contract to be fulfilled with the individual or they have asked you to take specific steps before entering into a contract. |
| Legal obligation | The processing is necessary for you to comply with the law. |

# Lawful basis for processing (2)

| Vital interest | The processing is necessary for you to protect someone's life. |
| --- | --- |
| Public task | The processing is necessary for you to perform a task in the public interest or for your official functions and the task has a clear basis in law. |
| Legitimate interest | The processing is necessary for your legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individuals' personal data which overrides legitimate interests. |

# Legitimate Purpose

- Specified, explicit and limited purposes.
- Privacy notices/ Terms and Conditions
  - Provide the data subject with this information **AND** be very clear.
- Further processing for archiving is permitted but is limited
  - Data has to be made anonymous.

# Data Minimisation

- Adequate, relevant and limited to what you need.
- A data mapping exercise will help identifying what you information you need
  - Privacy by design approach.
- Consider agreements with suppliers and data processors
  - You may strip out certain data before passing on the information.

# Accuracy

- Accurate and kept up to date.
- When profiling information you must ensure that the right decisions are made about a subject.
- Data subjects have a right to correct inaccurate data.
- Contact data subjects on a regular basis to request/check an update of information.

# Storage Limitations

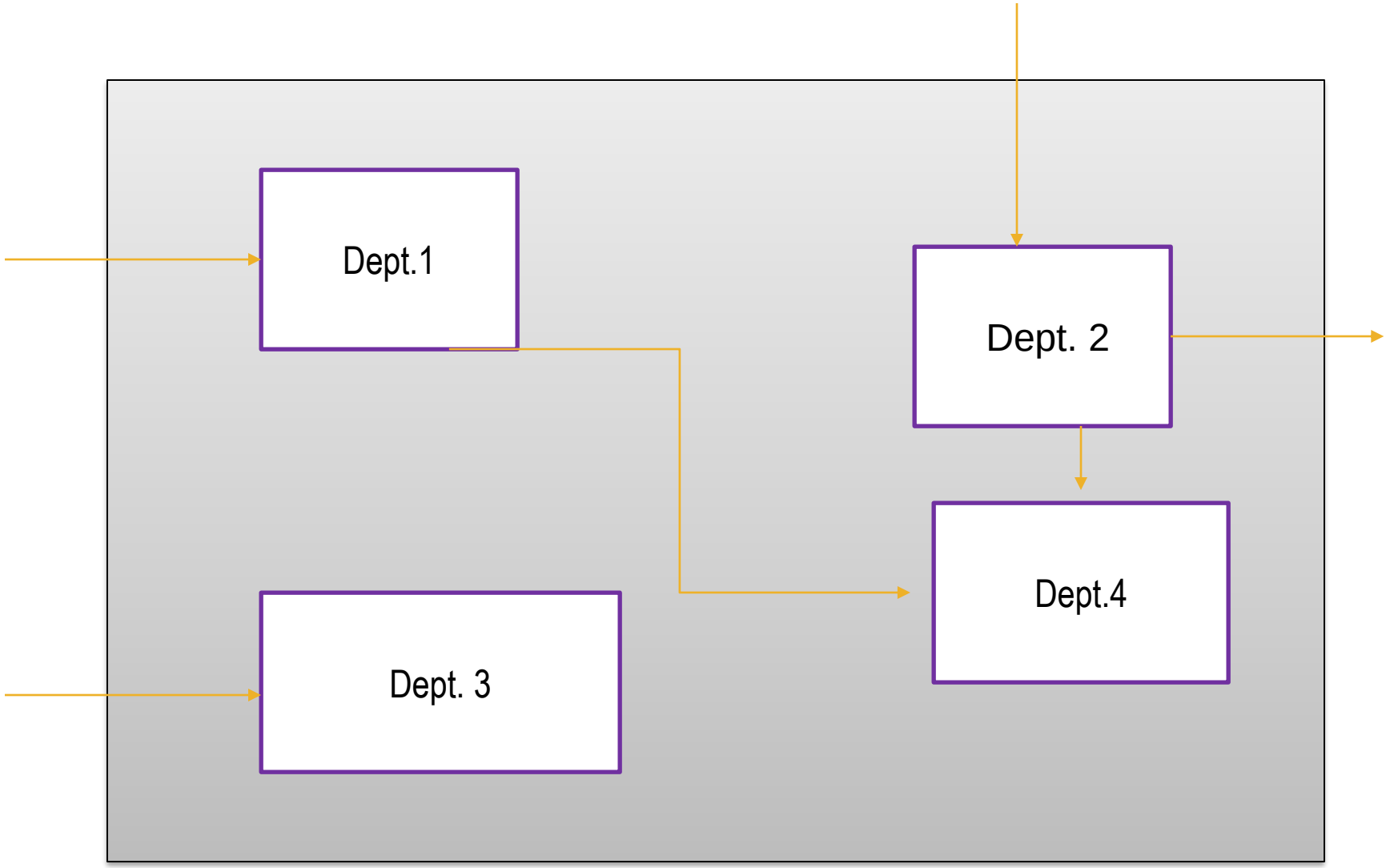
- Kept in a form which allows the identification of data subjects for no longer is necessary.
- Refers to the way in which it is stored
  - If you don't need it - then get rid of it.
- Define a purpose for the data.  Collect and then define when the data is no longer needed.
- Data retention policy
  - Take into account legal/contractual requirements.
- Make arrangements for deletion.

# Integrity and Confidentiality

- Process personal data that ensures the security of the data against unauthorised /unlawful processing.
- Personal data must be classed as confidential
  - Not all employees need access to it.
  - Integrity: property of accuracy and completeness
    - Data subject is not jeopardised by inaccurate information
    - Ensuring data is not corrupted over time by poor storage practices.

# Individual Exercise

- Take a sheet of Paper and draw a large box – make sure you have about 3cm gap between the edge of the box and the edge of the paper.
- Inside the box – draw more squares,  these represent your departments.
- Now identify what information flows into each department.  Some information will come from outside, some information will be transferred between departments.
- Identify what the information is
- Identify what information flows out of the organisation and to where.


Dept.1
Dept. 2
Dept.4
Dept. 3

# Data Mapping

- Best practice for any data protection programme.
- Can prove challenging for an organisation
  - Rare to keep a centralised map for all data collection and processing activities.
- Clear overview of the organisation's data processing activities.

# Objectives and Outcomes

- Identify and address potential privacy issues.
- Data mapping should record key aspects of data workflows
  - Identify specific risks to personal data.
- Recognise who is involved at each stage and who **SHOULD** be involved.

# Four Elements of Data Flow

- Data Items
  - The information itself: name, address etc.
- Format
  - The state in which the data items are stored.
- Transport methods
  - How data is moved: physically, fax, electronically.
- Location
  - Where data items are stored: physical and digital locations.

# Method of Data Mapping (1)

- Visual representation of information flow.

| Activity | Who | What | | | When | | | | Location | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Type | Source | Legal Basis | Originally | Updated | Retention period | Determined by | D Drive | Mobile |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

# Data Retention

- You cannot hold to data indefinitely
- You have decide what is a suitable period
- Guided by regulations/ industry best practise and plain common sense.
- You cannot hold onto information just because it might be useful to you in the future

# Individual exercise

- Select one department
  - Produce a very simple map for that department
  - Identify each piece of information that you collect about an individual
  - Identify how you got that information
  - Identify on what basis you are holding that information
  - Identify where the information is stored – NB this may be more than one location.
  - Decide on how long you can /should hold that information for and the reason for that holding

# Risk Management and DPIA

- A data breach should be an event on the corporate risk register.
- Data Protection Impact assessment.
- Estimate the following:
  - Likelihood of a data breach occurring given the existing mitigation.
  - Impact to Data subject and the organisation should a breach occur.
- Evaluate the risk
  - Implement a risk response to match the level of the net risk evaluated.

| What | | | When | | | | Location | | Risk Level | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Type | Source | Legal Basis | Originally | Updated | Retention period | Determined by | D Drive | Mobile | Controller or processor | Individual | Organisation |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

# Subject Access Request

- Enable the data subject to be aware of and verify the lawfulness of processing.
- Exercise right to obtain confirmation that their data is being processed by the Data Controller
  - Access to that data.
- One month timeframe.

# Receiving a request

- Any organisation that holds personal information could receive a SAR.
- Access request
  - Your process for the access request
  - Letter/email
  - High volume bulk requests.
- Could require you to return the information in a format that is not used by the organisation.

# How can data be lost or misused (1)

- Hardcopy
  - Stolen /seen from desktops/waste bins and unlocked cabinets.
- Electronic
  - Laptops/phones left on public transport/stolen from vehicles.
  - Information on unencrypted USBs.
  - Stolen in an hacking event – trojan horse or phishing event. Data is sold on.
  - Intercepted on a public or less secure Wi-Fi – to areas of the world where security isn't as good.

# How can data be lost or misused (2)

- Given away through an email or on the phone.
- The organisation uses information for purposes that are outside the scope of what they do.  For example;
  - You start selling perfumes or cars
- An employee leaves the organisation and takes the customer database with them and steals client details.
- Accidentally published on a website.

# Summary

- Key definitions of data protection
- Six principles of GDPR
- Lawful basis for processing information
- Importance of identifying what you have and how long you can keep it for
- How data can be lost

# Day 2

# Cyber security basics

The importance of cyber security in strategic risk management

# HUSHPUPPI

Let's start with a short video – Please pay attention to the narration

https://www.thenational.ae/uae/courts/instagram-celebrity-hushpuppi-extradited-to-the-us-after-arrest-in-dubai-1.1043211

# KEYWORDS

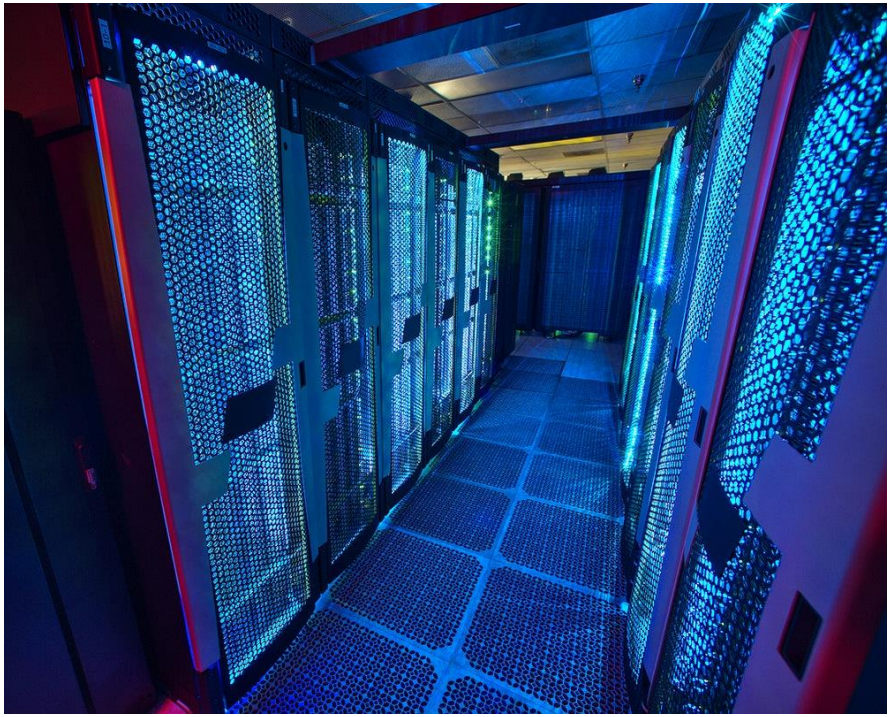
- Social Media
- Hacker
- Gang members
- Fraudulent activities
- Instagram celebrity
- Fraud charges
- Crimes committed in Different Parts of the World
- Successful businessman
- Wealth and expensive possessions
- Tracking every move
- Scammers
- Fake pages of existing websites
- Redirect victims' payments
- Hacking corporate emails
- Sending fake messages to clients - redirect financial transactions
- People's bank details
- Computers, smartphones, flash memory storage devices, Hard disks
- Almost 2 Million victims
- Luxury cars
- Cyber Criminals

# So…what is cyber security?

- Information Security OR Cyber Security
- Using the Internet as the main Threat Vector
  - Online Services
  - Information Hosted Online
- Protection against Cyber Criminals
- Technology vs Policy
- The Human Factor
  - Social Engineering
  - User Awareness
- Hacking

# what are we trying to protect?

- INFORMATION
  - Corporate Information
  - Strategic Information
  - Financial Information
  - Personal Information
- The Internet as the main Threat Vector
  - Online Services
  - Information Hosted Online
- What are our information assets?
- Which are our most critical assets? Why?



# THE CIA TRIAD

- The foundation of Information Security
- Confidentiality
  - Ensuring that only authorised users have access to specific information assets
- Integrity
  - Ensuring that data has not been tampered with and can be trusted
- Availability
  - Ensuring that authorised users retain access to information when needed
- Any cyber security incident violates one or more of these principles

# THE CIA TRIAD - CONFIDENTIALITY

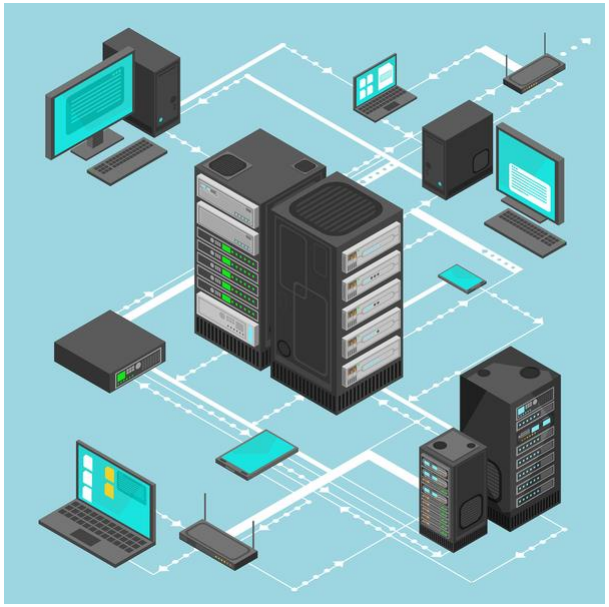
- Keeping data privacy and secrecy
- Prevention of unauthorised access
- Sometimes assumed but not guaranteed
- Systems and processes
- Fine-grained access control policies
- Confidentiality breaches:
  - Attacks to gain unauthorised access
  - Leaked user credentials

# THE CIA TRIAD - INTEGRITY

- Making sure that data can be trusted
- Prevention of data tampering
- Protecting data…
  - In use
  - In transit (email, uploads, downloads…)
  - In storage (on servers, in the cloud, …)
- Systems and processes
- Integrity breach can be…
  - Malicious (attacks)
  - Unintentional (Human error)
- Non-repudiation

# THE CIA TRIAD - AVAILABILITY

- High-value information needs to be available for access whenever required
- The need for timely, reliable access to resources when they are needed
- Protection from…
  - Hardware and software failure
  - Power failure
  - Natural disasters
  - Human error
- The need for…
  - Hardware fault tolerance
  - Regular software patching
  - Disaster Recovery Plans



# Common cyber security threats

## Complexity of modern businesses

- Email
- Mobile devices
- Corporate website
- Social media
- Ecommerce systems
- Online banking
- BYOD and office policy
- Network management
- Backup and remote access

# COMMON cyber security threats

**Phishing Attacks, Ransomware, Hacking, Imposter Scams & Environmental events**

## Phishing attacks

- Social engineering attack involving trickery
- Designed to gain access to systems or steal data
- Targeted phishing is "spear phishing"
- Variants include "vishing" – attacks by telephone and "smishing" those using SMS or text
- How do you protect against it?

# Ransomware

- Type of software with malicious intent and a threat to harm your data
- The author or distributor requires a ransom to undo the damage
- No guarantee the ransom payment will work
- Ransom often needs to be paid in cryptocurrency
- How do you protect against it?

# Hacking

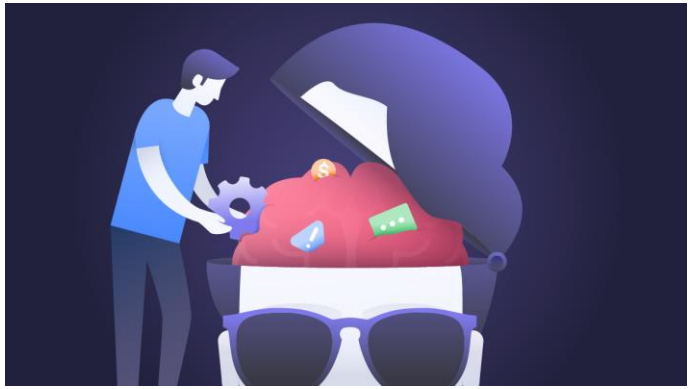
- **Unauthorized access to systems and information**
- **Website attack such as DDOS**
- **Access denied to authorized users**
- **Stolen funds or intellectual property**
- **How do you protect against it?**

# Environmental threats

- **Natural threats such as fire, earthquake, flood can cause harm to computers or disrupt business access**
- **Recovery efforts attract scams such as financial fraud**
- **Downtime can lose customers, clients who can't wait**
- **How do you protect against it?**

# Social engineering

- Someone “official” calls or emails to report a crisis situation
- They represent the IRS, a bank, the lottery or technical support
- There will be a sense of urgency and a dire penalty or loss if you don’t act
- How do you protect against it?



## Cyber security and erm

- Cyber Security is a problem that will never be solved
- Cyber Security is a risk to be managed
- Cyber risk is an issue for the entire business, not just the tech guys and IT
- Executives need to look at Cyber Risk from a business perspective
- To evaluate Cyber Risks, one must understand the impact they have on the organization
- When analysing Cyber Risk, it has to be done within the relevant business context to effectively prioritise risks
- With the increasing reliance on technology, Cyber Security has become essential to comprehensive Enterprise Risk Management (ERM)

# Cyber security risk assessment

1. Identify and Prioritise your assets
2. Identify Threats
3. Identify Vulnerabilities
4. Analyse Controls
5. Determine the Likelihood of an Incident
6. Assess the Impact of an Incident
7. Prioritise your Risks
8. Recommend Controls
9. Document the Results

# Cyber security risk assessment Identify & priorities assets

1. Identify Information Assets

- Business-critical information
- Client-sensitive Information
- HR & Payroll Information
- ERP Systems
- CCTV recordings

2. What systems host these assets?

3. Is anything hosted on 3rd Party Systems?

4. Prioritise according to:
   - Monitary value
   - Criticality to Operations
   - Regulatory and Compliance requirements

# Cyber security risk assessment - Identify threats

1. System Failures
2. Malicious software
3. Hacking attacks
4. Human Error
5. Natural Disasters

## Cyber security risk assessment - Identify vulnerabilities

1. Penetration testing (for unconfigured and misconfigured security systems)
2. Vulnerability scanning (for unpatched software and operating systems)
3. Physical Security Vulnerabilities (e.g. Unlocked Data Center)
4. Refer to NIST Vilnerability Database (https://nvd.nist.gov/)

## Cyber security risk assessment - ANALYSE existing controls

1. Analyse existing efforts to Control (e.g. Installed Firewalls, AV software…)
2. Security policies
3. Disaster Recovery and Contingency Plans

## Cyber security risk assessment determine the likelihood of an incident

The capability and motivation of the threat source

+

The existence and effectiveness of your controls

# Cyber security risk assessment assess the impact of an incident

- Assess Impact according to:
  - Monitary loss
  - Impact on Operations
  - Regulatory and Compliance requirements
  - Reputational Loss
- Make use of existing Business Impact Analysis exercises

# Cyber security risk assessment priorities cyber security risks

- The Level of Risk is determined according to:
  - The Likelihood that the threat will exploit the vulnerability
  - The Impact of the threat successfully exploiting the vulnerability
  - The adequacy of existing controls to reduce (or eliminate) such risk

- A Risk Matrix should be utilized to assist in this exercise

  LOW; MODERATE & HIGH

## Cyber security risk assessment RECOMMEND CONTROLS

- Mitigation Controls should take the following into consideration:
  - Organisational Policies
  - Company Objectives
  - Cost-benefit Analysis
  - Operational Impact
  - Regulatory compliance

## Cyber security risk assessment document results

- Risk assessment report should be presented to senior management
- Mitigation Controls should be endorsed by senior management
- The Risk Assessment Report is a live document
- Implementation of Controls should be given deadlines and audited

# Never too late to start

**Time to roll up our sleeves**

# Three main points…

1 – YOU NEED TO DO SOMETHING!

2 – THERE IS A LOT TO DO

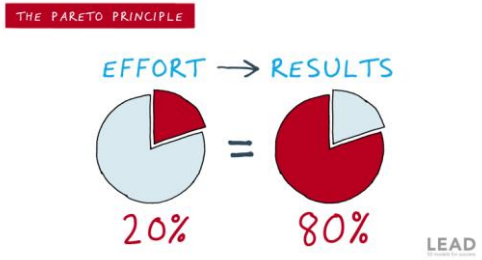
3 – THERE IS A LOT OF HARD WORK

## THERE IS A LOT TO DO

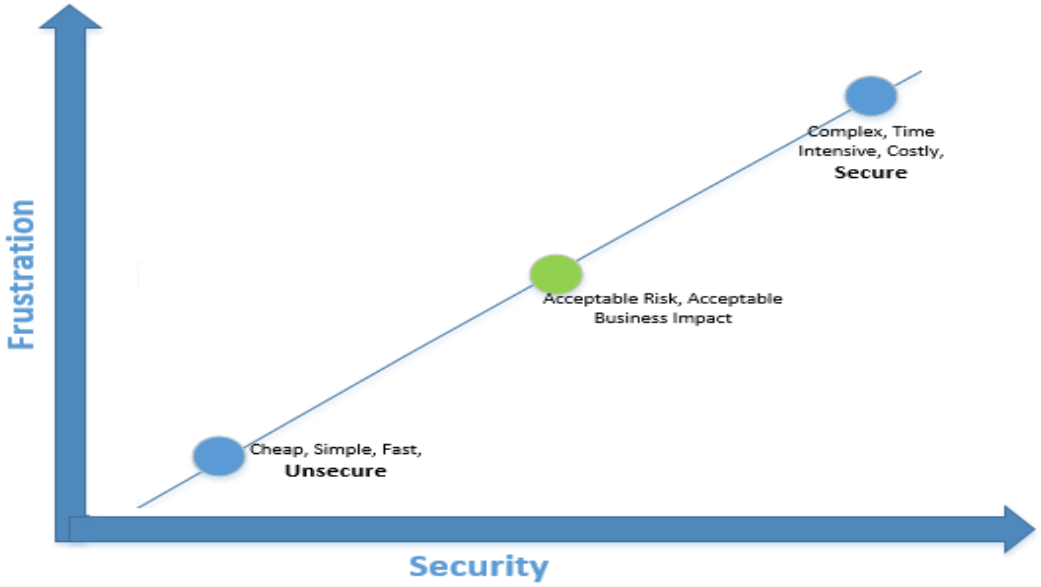

Stop saying - I'm not technical

Common sense security

The 80/20 rule or Pareto principle



# It is a lot of hard work!




## It is a lot of hard work!

Its as hard as you make it

The car analogy

Be more paranoid

# Cyber security guidance

5 STEPS TO GET YOU STARTED:

1. BACKING UP YOUR DATA
2. PROTECTING YOUR ORGANISATION FROM MALWARE
3. KEEPING YOUR MOBILE DEVICES SAFE
4. USING PASSWORDS TO PROTECT DATA
5. AVOIDING PHISHING ATTACKS

## BACKING UP YOUR DATA

1. IDENTIFY WHAT DATA YOU NEED TO BACK UP
2. KEEP YOUR BACKUP SEPARATE FROM YOUR COMPUTER
3. CONSIDER THE CLOUD
4. CONSULT ON CLOUD SECURITY
5. MAKE BACKING UP PART OF YOUR EVERYDAY SECURITY

## PROTECTING YOUR ORGANISATION FROM MALWARE

1. INSTALL ANTIVIRUS SOFTWARE
2. PREVENT STAFF FROM DOWNLOADING DODGY APPS
3. KEEP ALL YOUR IT EQUIPMENT UP TO DATE
4. CONTROL HOW USB DRIVES CAN BE USED
5. USE A FIREWALL (AND MANAGE IT PROPERLY)

## KEEPING YOUR MOBILE DEVICES SAFE

1. SWITCH ON PASSWORD PROTECTION
2. MAKE SURE LOST OR STOLEN DEVICES CAN BE TRACKED, LOCKED AND WIPED
3. KEEP YOUR DEVICE UP TO DATE
4. KEEP YOUR APPS UP TO DATE
5. DON'T CONNECT TO UNKNOWN WI-FI HOTSPOTS

## USING PASSWORDS TO PROTECT YOUR DATA

1. MAKE SURE TO SWITCH ON PASSWORD PROTECTION
2. USE TWO-FACTOR AUTHENTICATION
3. AVOID USING PREDICTABLE PASSWORDS
4. HELP YOUR STAFF COPE WITH "PASSWORD OVERLOAD"
5. CHANGE ALL DEFAULT PASSWORDS

## AVOIDING PHISHING ATTACKS

1. CONFIGURE ACCOUNTS TO REDUCE THE IMPACT OF SUCCESSFUL ATTACKS
2. THINK ABOUT HOW YOU OPERATE
3. CHECK FOR THE OBVIOUS SIGNS OF PHISHING
4. REPORT ALL ATTACKS
5. CHECK YOUR DIGITAL FOOTPRINT

# The fugle!



You are the CIO of a global organization called The Fugle, on the verge of making the first release of a biometrically authenticated mobile payment app. You will steer the project through its final stages, dealing with your internal security team, your colleagues in Marketing and PR and of course your CEO.

http://targetedattacks.trendmicro.com/index.html

- Source: Raconteur: http://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/
- NIST: National Institute for Standards and Technology (US – nist.gov)
- Trend Micro Cyber Security Solutions – www.trendmicro.com
- ISACA – www.isaca.org

Planning your next retreat?
Take advantage of our

# Virtual Year-end Retreat Service

We Plan | We Deliver

With our Virtual year-end retreat service, you can now enjoy

1. **Improved Efficiency**
   Achieving the same thing at a lower cost
2. **Improved Productivity**
   Achieving better results at a lower cost
3. **Improved Effectiveness**
   Achieving improved results at the lower cost
4. **Improved Engagement**
   Achieving more staff engagement and ownership at a lower cost

Extra: Moremi Edutainment
(Interactive Risk Edutainment Workshop for Strategy and Performance Improvement).

Talk to us on +2348095550641
info@conradclark.com | www.conradclark.com

Conrad Clark Nigeria...helping you to succeed

STRATEGY, PERFORMANCE, RISK & TEAM BUILDING WORKSHOP

conrad clark
inspiring ~~im~~possibilities

# RISK APPETITE, CULTURE AND REPORTING

(Virtual Workshop)

**Fee: #35,000**

**Duration: 2days**

**Time: 9am -12noon** (Daily)

FOR BOOKINGS

CALL 0812 031 8671 | 0809 555 0641

EMAIL TO INFO@CONRADCLARK.COM

*For your*

# Risk Assurance & Corporate Governance Compliance

Talk to us on +2348095550641
info@conradclark.com
www.conradclark.com

Conrad Clark Nigeria...helping you to succeed


go.rims.org/CCN

**Conrad Clark Nigeria (CCN) Ltd**
**7th floor Mulliner Towers, 39 Alfred Rewane Road , Ikoyi, Lagos**
**Tel: 08095550641; +44 07551322077**
**Web: www.conradclark.com E-mail: info@conradclark.com**
**Twitter: @risk_pals**