Trainer: Ms. Brencil Kaimba (CISA|LPT|CEH|CEI|ISO 27001)

Content

Topic 1: Document Security

- ❑ **How do you process data?**
- ❑ **Data security needs for different industries**

Topic 2: Forensic audit (investigation)

- ❑ **Forensic Audit Process**
- ❑ **Evidence preservation**

Topic 3: Way-forward for CPA's

- ❑ **How do you defend yourself professionally when implicated?**
- ❑ **What's the impact of Forensic audit to your career?**

Topic 4: Q&A

Document Security - Introduction

When a company uploads its documents onto the internet through cloud storage devices and platforms, they are at an extremely high risk of falling prey to malicious viruses and dangerous hackers. When placed in a physical form, there is an extremely high chance that they can be **lost or damaged** due to consequences like fire or theft.

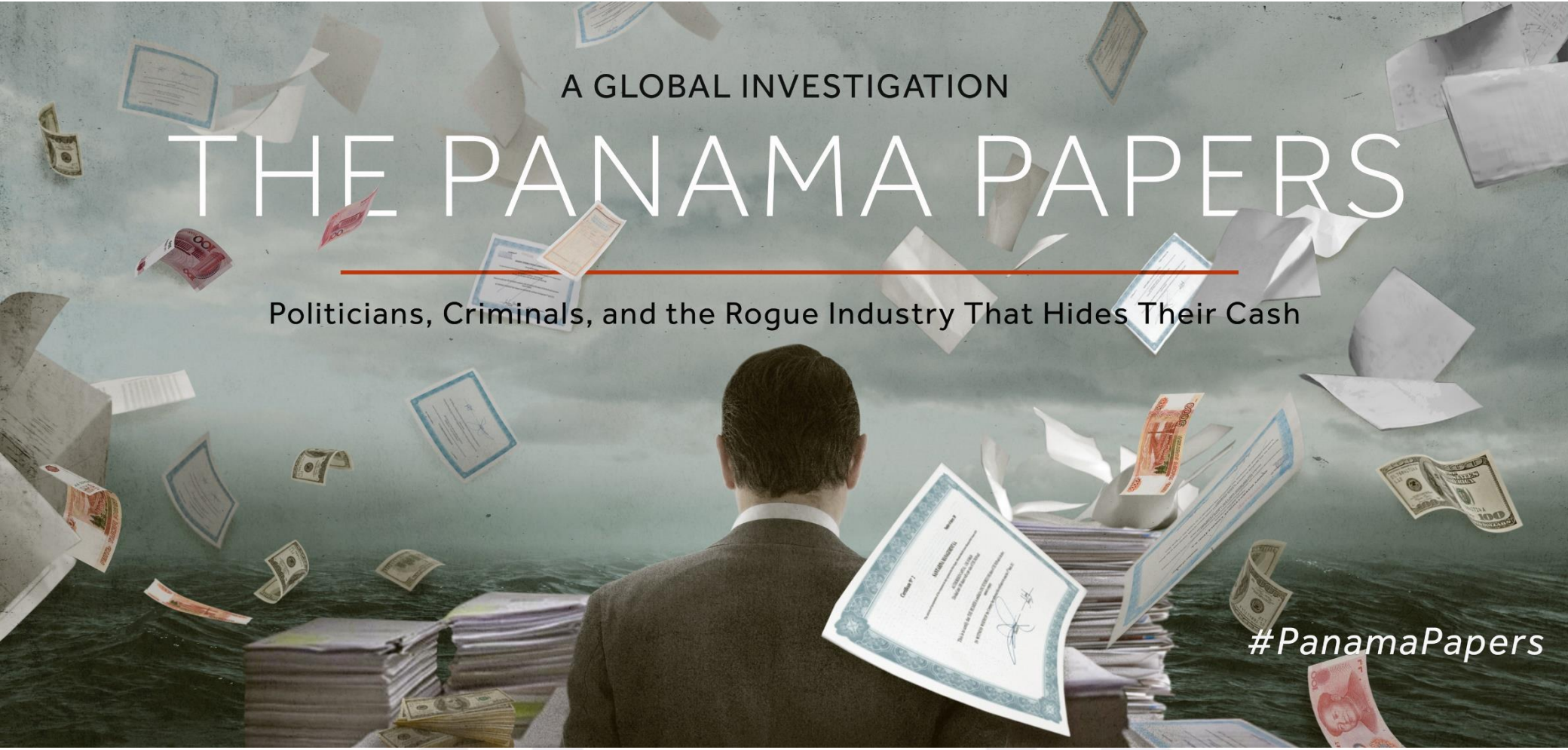
MEDIA AND TELECOMS APRIL 28, 2016 / 8:18 PM / UPDATED 5 YEARS AGO

Hackers leak stolen Kenyan foreign ministry documents

By George Obulutsa

4 MIN READ

NAIROBI (Reuters) - Online activists who claim ties to Anonymous said on Thursday they had begun to leak documents from Kenya's foreign ministry as part of a campaign to expose government and corporate corruption across Africa.


A GLOBAL INVESTIGATION
THE PANAMA PAPERS
Politicians, Criminals, and the Rogue Industry That Hides Their Cash
#PanamaPapers


Web...
Bing
Newspapers
view source
WikiLeaks
... could become as important a journalistic tool as the Freedom of Information Act.
— Time Magazine
Browse by
Country · Region · Language · Year
Submit documents

Document Security – Key Threats

HUMAN ERRORS

&

INSIDER THREAT

NATURAL CAUSES

DATA THEFT

&

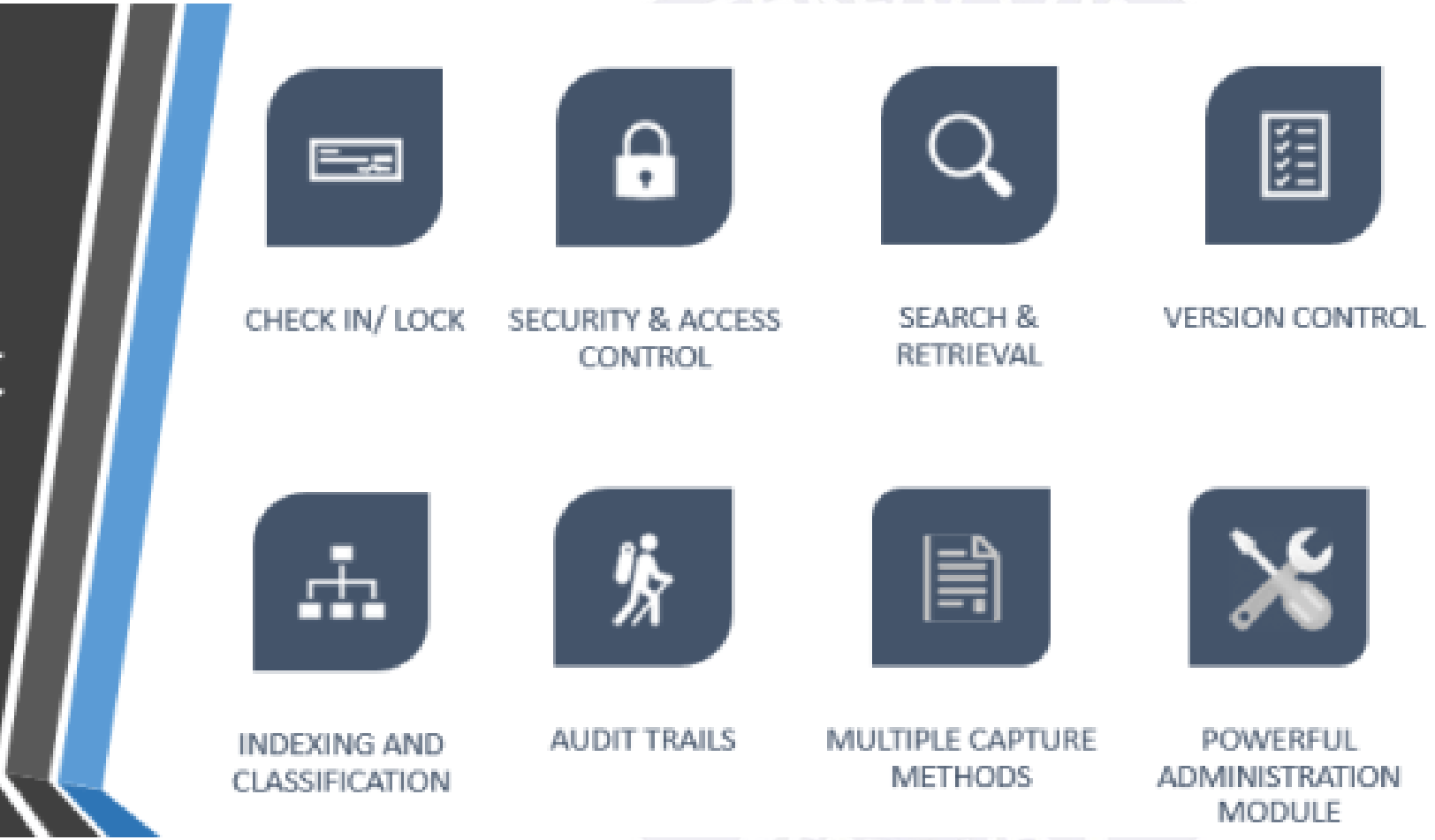
SECURITY BREACHES

Document Security – Scenario

Industry	Details
Hospital	**Key documents:** Medical personal data of patients **Risk:** Unauthorized access and manipulation **Impact:** Fines, Business closure.
Bank	**Key documents:** Account details of customers **Risk:** Unauthorized access and manipulation **Impact:** Rogue transactions, Fines from regulator, Business closure.

THE THREE DOCUMENT SECURITY FEATURE LEVELS

Document Security – Using a Document Management Tool



- Blackberry Workspace.
- One drive
- Google Workspace
- SharePoint (No encryption)

Content

Topic 1: Document Security

- How do you process data?
- Data security needs for different industries

Topic 2: Forensic audit (investigation)

- **Forensic Audit Process**
- **Evidence preservation**

Topic 3: Way-forward for CPA's

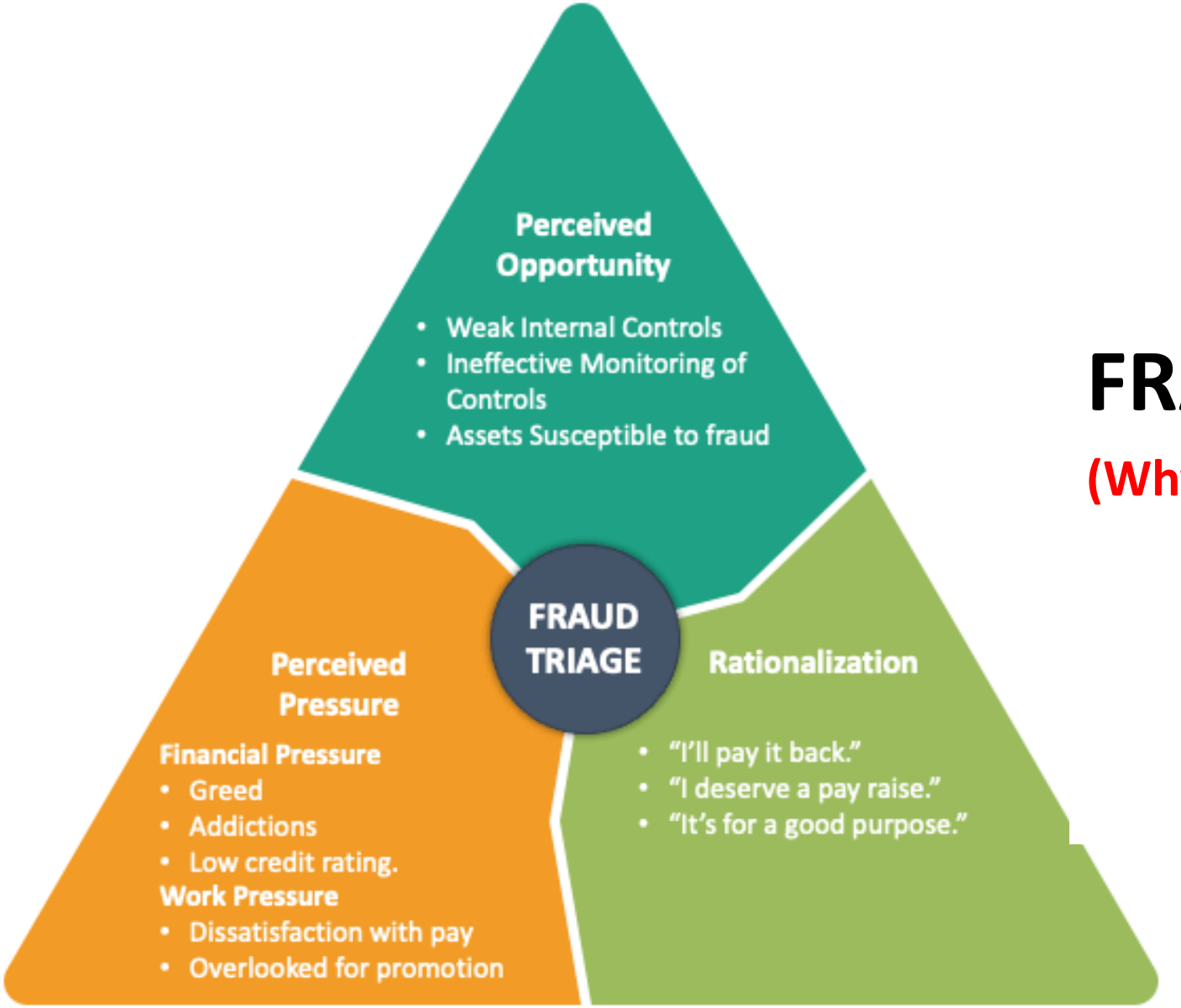
- How do you defend yourself professionally when implicated?
- What's the impact of Forensic audit to your career?

Topic 4: Q&A

Content

- According to estimates, employee fraud is a **$300 billion** a year problem that until only recently has gone largely unreported.

SERIANU



FRAUD TRIAGE

(Why People commit Fraud)

Case #1: Microsoft database leaked because of employee negligence

What happened?

- Microsoft customer support database that contained 250 million entries accumulated over 14 years was exposed online for about 1 month.
- The database included support cases and details, emails and IP addresses of customers, customers' geographical locations, and notes made by Microsoft support agents..

What were the consequences?

- Potential Fines - Data protection laws were not enforced then..

Why did it happen?

- Microsoft employees misconfigured those rules and caused the accidental leak. Access to the database wasn't protected with a password or two-factor authentication. Also, the company could have reduced the detection time significantly by monitoring user records and reviewing activity with sensitive assets.

Case #2: GE employees stole trade secrets to gain a business advantage

What happened?

- Two employees of General Electric (GE) stole data on advanced computer models for calibrating turbines the company manufactured. They also stole marketing and pricing information for promoting this service.
- With the stolen intellectual property in hand, one of the employees started a new company and competed with GE in tenders for calibrating the turbines.

What were the consequences?

- Lost several tenders for turbine calibration to the new competitor. In 2020, after several years of investigation, the insiders were convicted and sentenced to prison time and $1.4 million in restitution to General Electric.

Why did it happen?

- GE employees downloaded thousands of files with trade secrets from company servers and sent them to private email addresses or uploaded them to the cloud. One employee also convinced a system administrator to grant him access to data he wasn't supposed to have access to. None of these malicious actions triggered a response from the GE cybersecurity system.

Case #3: Tax Refund Fraud by Employees

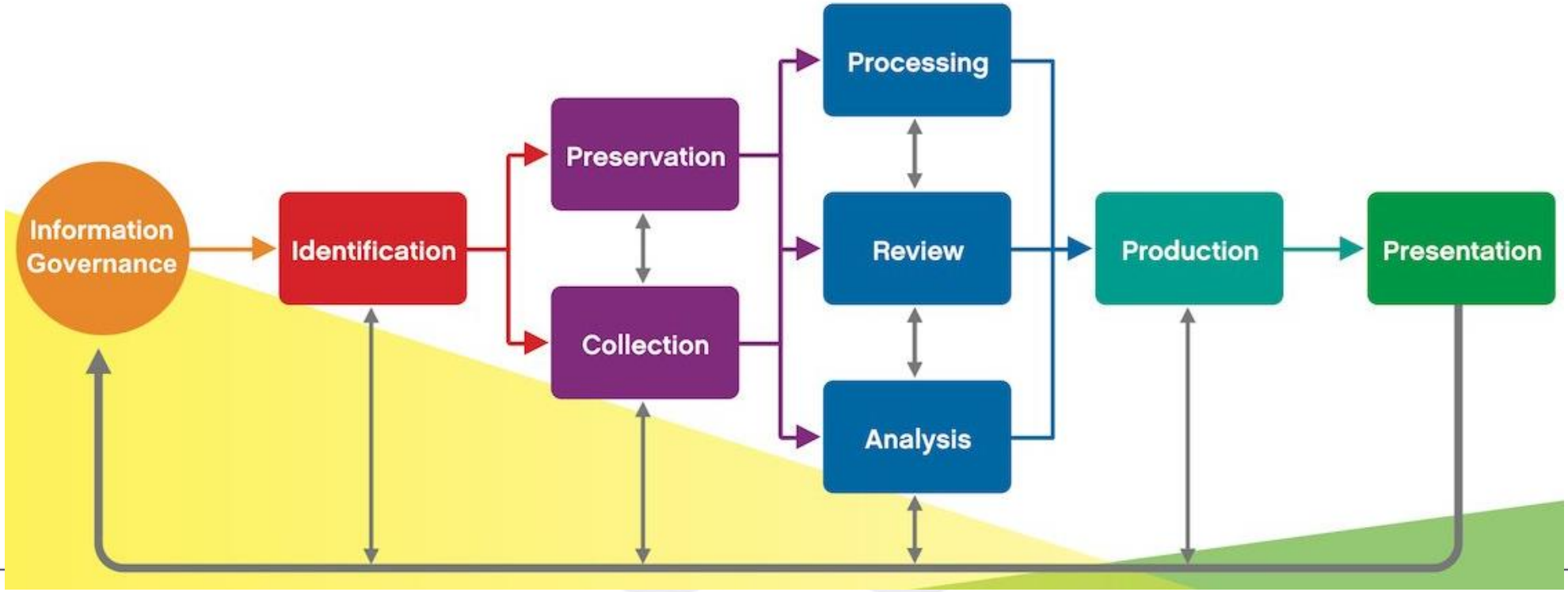
Accountants at a global firm were going through the refunds issued by a national call center. They found several discrepancies in the data

What happened?

- The call center employees at company X in are authorized to issue customer refunds of up to $50 without manager approval. The employees had been issuing refunds of between $30 and $40 and transferring the difference into their own bank accounts. The accountants found that more than 10,000 such fraudulent transactions were made over the course of the last few years.
- This is a great example of how fraud are being uncovered by accounting professionals at an increasingly frequent rate

EDRM Model

Electronic Discovery Reference Model (**EDRM**) creates practical global resources to improve e-discovery, privacy, security, and information governance.



SERIANU


Process of
Digital Forensics
What happens during a digital forensics investigation?
Identification
Preservation
Analysis
Documentation
Presentation

Practical Fraud Scenario Discussion

Review of common fraud scenarios…

FORENSIC GOLDEN HOUR – 10 TOP TIPS

- ❑Create your digital incident standard operating procedures sooner rather than later
- ❑Fully understand the legal scope of the incident. Never go further than your expertise will allow
- ❑Think beyond the device in question and consider paper documentation that might be in the office that should be protected as possible evidence
- ❑Keep copious and accurate notes of all your actions. Include full time and date information and use a bound note book, preferably with numbered pages

FORENSIC GOLDEN HOUR – 10 TOP TIPS

- ❑Remember to isolate equipment under examination from any network connection (Bluetooth, wired or wireless)
- ❑Never switch a device on if it is off
- ❑If a device is on and it appears to be actively deleting data or under external control consider powering it down by removing the power cord or battery. If possible take expert advice before doing anything.
- ❑Photograph and record external connections to the device such as printers or USB drives and any screen activities you can see
- ❑I[illegible] any associated equipment

Content

Topic 1: Document Security.

- How do you process data?
- Data security needs for different industries

Topic 2: Forensic audit (investigation)

- Forensic Audit Process
- Evidence preservation

Topic 3: Way-forward for CPA's

- **How do you defend yourself professionally when implicated?**
- **What's the impact of Forensic audit to your career?**

Topic 4: Q&A

- **How do you defend yourself professionally when implicated?**

- **What's the impact of Forensic audit to your career?**

Content

Topic 1: Document Security.

- How do you process data?
- Data security needs for different industries

Topic 2: Forensic audit (investigation)

- Forensic Audit Process
- Evidence preservation

Topic 3: Way-forward for CPA's

- How do you defend yourself professionally when implicated?
- What's the impact of Forensic audit to your career?

Topic 4: Q&A

Objectives and Scope

- Document security
  - How do you process data?
  - Data security needs for different industries:
    - Health (Security of Data)
    - Transport (Aviation)
    - Banking (Transactions)
  - Best practice for data security:
- Forensic audit (investigation)
  - What triggers Forensics Audit? Why is it different from other forms of Audit?
  - Forensic Audit Process
  - Evidence preservation
- Looking within:
    - How do you defend yourself professionally when implicated?
    - What's the impact of Forensic audit to your career?
    - What's your input as a CPA? What's ICPAK's code of conduct?


SERIANU CYBER-THREAT COMMAND CENTRE
SC3
ANTICIPATE • DETECT • RESPOND • CONTAIN