Cyber Incident Response
An integrated approach

Moniphia O Hewling PhD

Head – Jamaica Cyber Incident Response Team

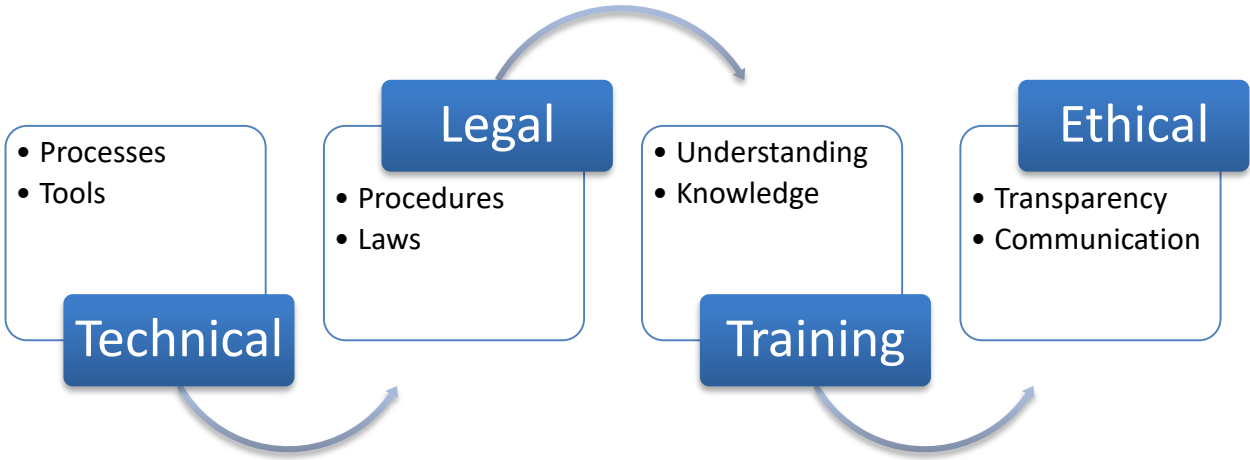
Rationale

- The need for Incident Response
  - Increased connectivity
  - Increase the number of reported cyber security related issues
  - Locating and identifying the source of cyber incidents

The Framework Outline

Major Area - Phases

Dimensions



The Framework [Core Principles]

C4. Practitioners should keep up to date with the developments in the field through training, workshops. Conferences and research publications. They should evaluate their performance regularly and be committed to

C6. Practitioners should be familiar with a variety of operating systems.

T2. Be aware of the limitations of the various digital forensics tools and strategies to overcome them.

E2. Know and understand the techniques used in a digital forensics examination.

$E_1$4. Ensure transparency throughout the process

L4. Know the different laws applicable to a digital forensic investigation.

		Legal (L)	**Educational (E)**	**Ethical (E_1)**
		be aware of e current legal quirements, tional/internat nal policies and idance garding pturing digital evidence. L2. Be aware of the legal documents required for use before, during and after the digital forensics process. L3. Create and maintain an audit trail in accordance with	E1. Have secure knowledge and exam E3. Know, understand and respect the roles of self, colleagues and other stakeholde E4. Have sufficie knowledge to be give advice on th different stages digital forensic investigation as w different tools used. E5. Knowledgeable on vestigative chniques used in the eld.	$E_1$1. Observe local and tional and nes when digital c ation. ow how to effectively communicate with teams members and $E_1$4. Ensure transparency throughout the investigation.
proving d				
titudes sional	limitations of e various digital forensics tools and strategies to overcome them. T3. Have sufficient depth of knowledge about the tools they use to be able to become expert witness T4. Know identify a address p with tool equipme they use to refer them.			

Framework [General Principles]

	Tools and Procedures	*Procedures*	*Certifications and qualifications*	*Roles and responsibilities*
Initiation (I_1) $I_1$1. Practitioners must observe the legal requirements for the authorization and capture of digital evidence. **$I_1$2. Practitioners must be cognizant of the expectations of all stakeholders.**	$TI_1^{\{1\}}$ Know the range of devices that may be involved in the investigation. **$TI_1^{\{2\}}$ Select appropriate tools based the digital devices to be encountered in the investigation**.	**$LI_1^{\{1\}}$Aware of legal requirements for the capturing of digital evidence.** $LI_1^{(2)}$ Select tools for the investigation in accordance with the recommended principles and guidelines.	$EI_1^{(1)}$Posses the educational background and capability to handle all aspects of the investigation. **$EI_1^{\{2\}}$ Select tools that the practitioner has been trained to use.**	**$E_1I_1^{\{1\}}$Disclose any conflict of interest with regards to the impending investigation**. $E_1I_1^{(2)}$Approach the investigation objectively.

Framework [General principles]

Investigation (I_2) **$I_2$1. Practitioners must adhere to guidelines to ensure sound retrieval of digital evidence**. $I_2$2. Practitioners must observe techniques to ensure preservation of digital evidence before, during and following acquisition. $I_2$3. Practitioners must ensure correct measures are taken to protect the scene of the incident.	$TI_2^{(1)}$Appropriate methods and techniques are used in accordance with the recommended guidelines. **$TI_2^{(2)}$Ensure tools used are clearly understood and can be used by another investigator and produce the same results**	$LI_2^{(1)}$Ensure that methods used can be reproduced by other investigators producing the same results. $LI_2^{(2)}$ Be aware of the laws associated with the investigation at this stage. **$EI_2^{(3)}$Treat all data and devices as potential legal evidence.**	$EI_2^{(1)}$Ensure that practitioner is trained to use the tools available where open source or commercial. **$EI_2^{(2)}$Ensure knowledge of the different tools to be used for different purposes throughout the examination.** $EI_2^{(3)}$Treat all data and devices as potential legal evidence. $EI_2^{(4)}$ Be Knowledgeable of the tools they work with and how they do what they do.	$E_1I_2^{(1)}$Maintain objectivity throughout the investigation $E_1I_2^{(2)}$Treat all data and devices as potential legal evidence. **$E_1I_2^{\{2\}}$Exercise care to ensure to ensure the integrity of the evidence acquired.**

Framework [General Principles]

Report (R)	TR[1] Archive all software tools used. **TR[2] Archive all hardware tools used**	LR[1] Document all hardware tools used in accordance with the recommended guidelines. **LR[2] Document all tools in accordance with the recommended guidelines**	ER[1] Practitioners must have sound knowledge in the reconstruction of a digital crime scene. ER[2] Practitioners must be knowledgeable in archiving and documenting tools used ER[3] Practitioners must adequately trained to produce a comprehensive report of the investigation. **ER[4] Posses training to interpret finding accurately** ER[5] Be knowledgeable in creating an attacker profile.	$E_1R^{(1)}$ Practitioners must ensure confidentiality in the findings of the investigation. **$E_1R^{(2)}$ Practitioners must ensure full disclosure of their findings to the relevant personnel.**
R1. Practitioners should ensure accuracy in classifying and reconstructing the incident scene. R2. Practitioners should be constructive in producing a relevant report. R3. Practitioners should recognize that this phase may include being an expert witness. **R4. Practitioners should be reflective and responsible for identifying drawbacks and facilitate ways for improvement.**				

JamaicaCIRT partners

- Communication Forensics and Cyber Crime Division
- Major Organised Crime Agency (MOCA Cyber)
- Office of the CIO

Jamaica's Framework to date

- National Cyber Security Strategy Launched in 2015
- Cybercrimes Act 2015
- Completion of Implementation Plan
- Launch of Public Education Campaign

THINK BEFORE YOU CLICK