Forensic Investigation on High Risk Assignments (Tips, Success and Failure Stories)

PRESENTED BY;

REUBEN BORO GITAHI

Determining the Physical Requirements for a Computer Forensics Lab

Most of your investigation is conducted in a lab

Lab should be secure so evidence is not lost, corrupted, or destroyed

Provide a safe and secure physical environment

Keep inventory control of your assets

- Know when to order more supplies

Identifying Lab Security Needs

Secure facility

- Should preserve integrity of evidence data

Minimum requirements

- Small room with true floor-to-ceiling walls
- Door access with a locking mechanism
- Secure container
- Visitor's log

People working together should have same access level

Brief your staff about security policy

Conducting High-Risk Investigations

High-risk investigations demand more security than the minimum lab requirements

- TEMPEST facilities
  - Electromagnetic Radiation (EMR) proofed
  - *http://nsi.org/Library/Govt/Nispom.html*
- TEMPEST facilities are very expensive
  - You can use low-emanation workstations instead

Using Evidence Containers

Known as evidence lockers

- Must be secure so that no unauthorized person can easily access your evidence

Recommendations for securing storage containers:

- Locate them in a restricted area
- Limited number of authorized people to access the container
- Maintain records on who is authorized to access each container
- Containers should remain locked when not in use

Using Evidence Containers (continued)

If a combination locking system is used:

- Provide the same level of security for the combination as for the container's contents
- Destroy any previous combinations after setting up a new combination
- Allow only authorized personnel to change lock combinations
- Change the combination every six months or when required

Using Evidence Containers (continued)

If you're using a keyed padlock:

- Appoint a key custodian
- Stamp sequential numbers on each duplicate key
- Maintain a registry listing which key is assigned to which authorized person
- Conduct a monthly audit
- Take an inventory of all keys
- Place keys in a lockable container
- Maintain the same level of security for keys as for evidence containers
- Change locks and keys annually

Using Evidence Containers (continued)

Container should be made of steel with an internal cabinet or external padlock

If possible, acquire a media safe

When possible, build an evidence storage room in your lab

Keep an evidence log

- Update it every time an evidence container is opened and closed

Overseeing Facility Maintenance

Immediately repair physical damages

Escort cleaning crews as they work

Minimize the risk of static electricity
- Antistatic pads
- Clean floor and carpets

Maintain two separate trash containers
- Materials unrelated to an investigation
- Sensitive materials

When possible, hire specialized companies for disposing sensitive materials

Considering Physical Security Needs

Create a security policy

Enforce your policy

- Sign-in log for visitors
  - Anyone that is not assigned to the lab is a visitor
  - Escort all visitors all the time
- Use visible or audible indicators that a visitor is inside your premises
  - Visitor badge
- Install an intrusion alarm system
- Hire a guard force for your lab

Auditing a Computer Forensics Lab

Auditing ensures proper enforcing of policies

Audits should include:

- Ceiling, floor, roof, and exterior walls of the lab
- Doors and doors locks
- Visitor logs
- Evidence container logs
- At the end of every workday, secure any evidence that's not being processed in a forensic workstation

Reuben Boro Gitahi

Olsen Partners

reuben.gitahi@one-source.info

Mobile:+254-722-372677

www.olsenea.com