When you discover that your enterprise has been breached, your initial thoughts go to solving the immediate problem. But for cyber forensic professionals, that is only the beginning. It is important for security professionals to undergo a thorough process of identifying, preserving, analyzing, and presenting digital evidence. To support this discipline, specialized tools have emerged to assist investigators in capturing, analyzing, and preserving evidence that might arise during the course of investigating criminal activity. We will be discussing the importance of formulating a digital forensic lab on an adequate budget that contains physical, hardware, software, and high-level criteria assessments to determine the best fit for this project.

The fundamental concept proof of great forensic lab testing comes from the heart of budget allocation. We can determine the total estimated costs by breaking down the cost into daily and annual sections. A great way to forecast the budget that varies for each individual/company can be by examining past investigations. Adding up the amount including software, storage tools, hardware, or overhead. Maintenance is another aspect to consider because hardware needs replacing once in a while. The software also demands upgrades and patching because new versions are constantly coming out. TCO(total cost of ownership) is a factor to consider for managers when paying out dividends to help a team configure an application properly. We must take in consideration for training team members/employees how to handle and extract data and evidence. Pondering about all the resources allocated to create the lab when making our purchase decisions. It renders our labs obsolete if the tools or technologies are not up-to-date and running. The availability of hardware should be ready when needed. Alongside software licensing must be purchased with the newest version. “Budget allocation for developing a forensics laboratory depends on the total estimated cost needed to meet the accreditation standards of a standardized body that certifies labs. In the area of forensic science, the American Society of Crime Laboratory Directors acts as a certifying body for crime labs. This standard also applies to computer forensics laboratories.”

“Don’t delay and give your digital forensics lab the overhaul it needs. Remember – this is not a cost, it’s an investment that virtually pays for itself through a higher case resolution percentage and winning the trust with your work.”

Physical controls are important steps to begin the operation. Finding a suitable environment into which we can input high-end forensic lab equipment. The basic concepts of physical security controls involved controlled access, evidence lockers, and control & climate humidity. Access to the lab must be maintained and controlled. This is to uphold the train of custody therefore only individuals with privileged access needs to be allowed in the lab space. This limits the necessary chances of evidence being tampered with or destroyed. Controlled access would also include access cards, key fobs, or coded key locks on doors will be great for keeping unauthorized personnel out of access to the lab. Evidence lockers are where evidence can be stored properly. They should also be secured with an onboard lock or key. This vital concept is so that there is the separation of cases is thoroughly organized. Climate, humidity, and ventilation controls should be taken into consideration when dealing with different locations and workstations throughout the lab. Having a cluster of employees residing in a small workstation can create an unhealthy exhaustive climate. Rendering proper airflow in the facility will comfortably help the environment. This will assist with keeping dirt and dust from polluting in the lab. Another reason for the high temperature can lead to hardware failure. “Before going further, you should remind that what you’re looking for is an environment that is clean, cool, and available – the last thing you want is to risk that the evidence ends up damaged due to unsuitable environmental factors.”

Tools specifically for hardware needed to complete the task at hand. Forensic workstations are used to perform the imaging of hard drives while processing large amounts of data. The workstation should have sufficient ram and processing power and should be set up with a hard drive containing the operating system. Having a backup power supply in case of emergency outrage will be a very prominent urgency. A recommended power generator and uninterrupted power supple(UPS) to protect from power shortage and loss of sensitive data in the lab. Alongside other tools needed to perform the task required would be an external hard drive and disk duplicator. In order to hold all the pieces of evidence, ensuring that the pieces of evidence are presented to complete the verification process. By making sure the data is copied and integrity is intact. We can proceed to store the information as a NAS. depending on the retention policies, we can further opt for tapes. In a company with a workstation, the lab should also have a research workstation with an internet connection. To conduct research or write reports. This specific workstation should never be made public on the internet. With further workstations, you also have to write blockers for they are critical to the forensic lab. This device allows for hard drives that have been seized to connect with forensic imaging machines. “Apart from the run-of-the-mill digital forensics equipment such as workstations, monitors, evidence storage, large displays, intelligent tables&chair, and similar, it’s a good idea to cover all your bases and have a well-rounded base of operations from where you’ll be conducting your investigation.” Finding the best hardware while on a budget can be promising. The selective hardwares should adequately provide atmosphere of comfortability, dynamic workload, and the ability to digress with different case of investigations. Recommended comprehensive protection kit that is use to collect and detect samples of evidence. Mounting projectors, flat screen monitors, or Tv’s throughout the lab to better assist workers as they dive into their analysis.

There is much software to choose from for the lab. Many of which are either paid or open-source. For application specifically, there are autopsy, EnCase, Forensic Toolkit, Magnet Axiom. Then there are software tools specific to the operating system case such as DEFT Zero, Paladin, CAINE, and Linux Forensic. Depending on what type of digital forensic labs you want to conduct will depend on which application and OS you will be utilizing. “Unless, of course, you’re planning to wing it by relying on open-source digital forensic tools exclusively. That, however, can have its fair share of drawbacks, the most notable of which is a steep learning curve, lack of support, hidden malware, data loss, and simply not being up to the modern day’s digital forensics challenges. As a general rule of thumb, you get what you pay for. If nothing else, paid digital forensics software is the superior choice due to the support that you get. As you probably know already, during an investigation, time is of the essence, and you simply cannot afford to lose any of it by having to stumble over technical hurdles.” SIFT is considered on the list as the workstation is an ubuntu-based distribution software that can run on a 64-bit operating system. Which entailed to engrossing more memory efficiently. Autopsy is a great windows based tool choice to inspect mobile phones and hard drives. An adverse software that is known to many includes up-to-date forensic tools, built-in timeline analysis, web artifacts, keyword searches, and much more. Another considerable software tool to use can be FTK. a very easy on-going tool to work with. That allows you to specify criteria, like file size, pixel size, and data type, to reduce the amount of irrelevant data. This tool can help with duplicating files and data without tampering with the originality of the evidence.

“There are four phases involved in the initial handling of digital evidence: identification, collection, acquisition, and preservation ( ISO/IEC 27037 ; see Cybercrime Module 4 on Introduction to Digital Forensics).” identification is process of obtaining the case information prior to the start of the lab report. “Digital evidence can be found on digital devices, such as computers, external hard drives, flash drives, routers, smartphones, tablets, cameras, smart televisions, and Internet-enabled home appliances.” The collection process involves making sure any physical piece of evidence is obtained at all cost. “The cybercrime crime scene also includes the digital devices that potentially hold digital evidence, and spans multiple digital devices, systems, and servers.” Performing acquisition is being able to exit smoothly and closing the cases. “The seized digital devices are considered as the primary source of evidence. The digital forensics analyst does not acquire data from the primary source. Instead, a duplicate is made of the contents of that device and the analyst works on the copy.” Perseveration process takes us into the look of maintaining digital integrity. “First responders, investigators, crime scene technicians, and/or digital forensics experts must demonstrate, wherever possible, that digital evidence was not modified during the identification, collection, and acquisition phase; the ability to do so, of course, depends on the digital device (e.g., computer and mobile phones) and circumstances encountered by them (e.g., need to quickly preserve data).”

Gregg, B. (2009, July 22). *How to build your own digital forensics lab, Cheap*. Computerworld. Retrieved February 22, 2023, from https://www.computerworld.com/article/2526019/how-to-build-your-own-digital-forensics-lab--cheap.html

*How to set up a digital forensic lab? （7 steps to approach）*. Salvation DATA. (2022, June 28). Retrieved February 22, 2023, from https://www.salvationdata.com/technical-tips/set-up-a-digital-forensic-lab/

Katharina.kiener-Manu. (n.d.). *Cybercrime module 6 key issues: Handling of digital evidence*. Cybercrime Module 6 Key Issues: Handling of Digital Evidence. Retrieved February 22, 2023, from https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html#:~:text=There%20are%20four%20phases%20involved,on%20Introduction%20to%20Digital%20Forensics).

Panhalkar, T. (2020, June 25). *Setting up a Computer Forensics Lab*. Infosavvy Security and IT Management Training. Retrieved February 22, 2023, from https://info-savvy.com/setting-up-a-computer-forensics-lab/