INTRODUCTION

Red teams are external units that evaluate the effectiveness of a security program. It is achieved by simulating the behavior and methods of possible attackers in the most convincing manner. Blue teams are integrated security groups that protect the organization from real attackers and the Red Teams. Since many security teams are not constantly attacked, most Blue Teams should be separated from established standard security groups (Miessler, 2016).

Red Team and Blue Team exercises were named after similar military experiences. The concept is that a group of security experts (the Red Team) is attacking an object, and the other group (the Blue Team) is protecting them. Initially, the exercises were run by the army for military training. They have also been utilized to assess the physical security of high value assets, such as nuclear facilities.

According to Hargreaves and Chamberlain (2018), Red Teams have been hired to replicate the behavior and methods of the attackers in the most realistic possible way. For instance, this group may attempt to enter a commercial building by acting as a distribution controller in order to configure the device to facilitate public access. On the other hand, the Blue Team is responsible for defending against these attacks, and functions as the internal security team. The Red Team is generally security goal oriented and tries to secretly verify the company's own defense. The team involves well-trained and technically competent security experts, whose goal is to ascertain and take advantage of security vulnerabilities in the system (CybeRisk, 2018).

Miessler (2016) argues that, excluding complex threats in the real world, the exercise will be very realistic. Red Team is not limited to IT tools and advanced technology to penetrate systems and buildings. It can include writing a personal malware and developing new methods, just as spiteful hackers do. Everything is allowed including social engineering and psychological manipulation to achieve their goals. If they need to mask their entry by posing as the courier to connect the USB device to a computer, so be it. The Blue Team is usually the company's
Director of Security at the Security Operation Center (SOC). SOC is made up of very qualified analysts who protect and improve the security of the organization 24x7.

Drinkwater and Zurkus (2017) point out that the Blue Team must determine, defend and weaken the Red Team. The attack simulation is intended to improve their capabilities by organizing them for dangerous attacks in the real world. Blue Team will identify and defuse the most demanding attacks and carefully monitor contemporary and evolving threats to the active protection of the company.

**SHOULD DIGITAL FORENSICS BE OUTSOURCED WITHIN GOVERNMENTS AND/OR FEDERAL INSTITUTIONS**

Digital Forensics operates as part of the Blue Team, since it works as part of the SOC or the Computer Security Incident Response Team (CSIRT). Generally, not everything is included, but it has the background of the Security Operations Center. Digital Forensics requires tools to check deleted files in hard disks, memory, browser caches and Windows registry (Paganini, 2016).

There are two sides to the argument; one says outsource all you can for whatever resources and competences needed. The other says do not outsource critical functions which compromise your most valuable assets.

**ARGUMENTS FOR OUTSOURCING**

Evans (2016) points out that computer forensic reviews are generally performed inadequately in many medium and large institutions. Even though the current trend includes computer forensics as an integral discipline of an extensive information security program, there are several institutions with limited capability for computer forensics.

Devlin (2018) argues that if the institution has conflicting legal requirements or cannot provide a permanent source of support for this resource, it is reasonable to transfer it to a third party. Outsourcing solutions must be based on the required IT skills and, of course, on cost analysis. The organization must also determine the scope and possibility of the possible outsourcing contract, as well as the internal resources needed to attain the required capacity level.

Devlin (2018) indicates that there are four main reasons for this inconvenience: computer forensic examinations and their assistance activities are very costly, complex and technically complex with possible legal consequences; new tools and methods with constant updates are
usually required to adapt to new technologies and threat models; it may be hard to validate the establishment and maintenance of a legal laboratory that will continue the process of collecting all the notches and is based on the burden of proof; and the protection of this capacity requires the development and formation of a large number of people.

The lack of specialists, such as digital forensic investigators, is a real problem. The analysis of any digital data is annoying and time-consuming, even with the aid of a specialized software. Digital forensics requires the analysis of multiple digital devices and the numbers can run into tens and hundreds, but there are not sufficient investigators to perform the necessary analysis. Digital forensic experts also have to deal with situations where they are limited in the number of hours that can be spent watching each hard drive. For each machine, it may take several days for proper legal work, requiring compliance to various standards and regulations, when dealing with a continuous flow of data entering the lab. Thus, their research work suffers (CYFOR, 2018).

ARGUMENTS AGAINST OUTSOURCING

There would be a number of instances that an organization would be compelled to seek the services of forensic experts in-house (Digital Discovery, 2011). While there are advantages of seeking the services of forensic experts in-house, there may be valid reasons that could limit federal institutions and government organizations from seeking these services. These situations include circumstances such as when the organizations are involved in legal law suits, where the organizations deals with classified materials, and even circumstances where the organizations experience frequent intrusions (Obbayi, 2018). Chain of custody can be compromised where the transfer of digital evidence is not documented, something that is more likely when digital forensics is outsourced. According to Devlin (2018), the one key advantage of seeking forensic experts in-house is the fact that it will go a long way in saving money. But saving cost is not a good enough reason to outsource your most critical functions.

Federal and government bodies have massive amounts of sensitive data that needs to be kept secret at any cost (Comtact, 2017). Devlin (2018) point out that choosing an in-house cyber security expert to secure critical data is a natural option. Many times it is difficult to ensure that the outsourced party is really as good as they claim to be. Furthermore, forensic experts in-house could play a continuance role in assisting to detect and investigate cases of fraud, asset misappropriation, abusing and misusing the system, and other forms of non-compliance.
CONCLUSION

The Red Team is under the organization's radar, while it targets its objectives without any limitation of time or resource. The Blue Team, on the other hand, needs to operate within organizational boundaries while being ever ready to defend against any attack. While they may be saving the organization against numerous attacks, one incident of security breach is enough to tarnish their image.

In the world cup, the game is not about how many balls the goalkeeper has defended, and no-one will remember this; it is about how many balls the goalkeeper missed, and this is what everyone will remember.

On another note, people will always remember the doctor whose negligence cost someone's life, but conveniently forget the thousand lives the doctor saved in his or her lifetime. This just highlights the tremendous pressure the Blue Team works under, every day of the year and especially the role that forensic experts in-house could play.

The courts place immense value to the integrity of digital evidence. Therefore, one cannot understate the importance of documenting the collection, examination, storage and transfer of digital evidence by competent people. Organizations need to assess the risk of outsourcing digital forensics aligned with these requirements.

The oft-quoted reason for outsourcing digital forensics is the lack of internal expertise, or to simply save money. Imagine if the hospital you visit does not have its own doctors, and shares all your medical information with an external consultant who prescribes your treatment. Would you go to such a hospital to save a few hundred dollars?

REFERENCES


