Exercise - Not Just for Your Body Anymore

Simulations and exercises have long been a tool that managers have had available to them to help keep staff in shape. The military is potentially the most proficient in using exercises to maintain skills through practical application in as close to real world situations as possible. In this paper, background on the evolution of cyber exercises and possibilities will be discussed. A variety of cyber exercise options will be detailed, including an analysis of the business impacts, risks and benefits that an organization ...

Exercise – not just for your body anymore

A comparative examination of the types of cyber exercises possible

GIAC (GSLC) Gold Certification

Author: Jonathan Risto, jonathan.risto@hotmail.com
Advisor: Kees Leune

Accepted: January 20th, 2015

Abstract

Simulations and exercises have long been a tool that managers have had available to them to help keep staff in shape. The military is potentially the most proficient in using exercises to maintain skills through practical application in as close to real world situations as possible. In this paper, background on the evolution of cyber exercises and possibilities will be discussed. A variety of cyber exercise options will be detailed, including an analysis of the business impacts, risks and benefits that an organization will need to weight prior to conducting. Areas requiring special attention from a management perspective will be described to help ensure success. A comparative analysis of the options will be presented to provide a quick reference of the material within the paper.

1. Introduction

Exercise programs have been publicized and encouraged for a long time as a way to keep your physical and mental abilities in shape. (Penedo & Dahn, 2005) (Cotman, Berchtold, & Christie, 2007) (Paffenbarger Jr, Blair, Lee, & Hyde, 1993). This improved physical and mental wellbeing helps to better prepare your body and mind for future challenges. The military uses exercises to teach new skills, hone existing skills, and maintain battle readiness. (Harris, 2014) (Skripnichuk, 2014) These exercises help ensure troops are able to react as quickly as possible.

So, exercise is good for you. Your first thought/question may be: Yeah, so what? What could this possibly have to do with cyber security and security management?

According to the Federal Emergency Management Agency's Emergency Management Institute, an exercise is "a focused practice activity that places the participants in a simulated situation requiring them to function in the capacity that would be expected of them in a real event. Its purpose is to promote preparedness by testing policies and plans and training personnel." (Federal Emergency Management Agency, 2014). Similarly, Merriam Webster's definition of exercise is "something that is done or practiced to develop a particular skill" (Merriam-Webster, 2014).

For numerous years, the military (NATO, 2014) (Carr, 2014), the government (Department of Homeland Security, 2013) (Davis & Magrath, 2013), academia (University of Hawaii Manoa, 2014), and industry (ANC R&D, 2014) (LohrMann, 2014) have utilized cyber exercises to further mature their abilities in the cyber security area through these learning opportunities. (Augustine & Dodge Jr, 2006) These activities have provided valuable lessons for the participants regarding skills shortages, procedural or policy deficiencies within their organizations or in cross-organization coordination and communication. (Branlat, Morison, & Woods, 2011) The shortcomings and lessons learned, in the case of government, have been reported and continue to be implemented. (United States Government Accountability Office, 2008) (European Union Agency for Network and Information Security, 2012)

I would argue that exercises are very important for cyber security and that some of the following organizational questions need to be asked:

- What is your organization doing in the area of cyber security exercises?
- Does your organization have any exercise identified to be performed within the next 1 year? 3 years?
- Does your organization perform a variety of exercise types?
- Does the senior leadership of your organization even know about or want to see the reports from these exercises?
- Or even the broader question of: What are we doing to improve our organizational security posture?

Within this paper, the definition of a cyber exercise will be provided. Following, numerous cyber exercise types will be presented and discussed. The general goals for each are offered with the high level requirements needed for each exercise type. The benefits and drawbacks of each type of exercise are conferred with a emphasis on the management implications, impacts and risks. Finally, the reasoning behind why senior leadership should want to see the outputs will be discussed.

2. What exactly IS a cyber exercise?

Just what IS a cyber exercise? What are the goals? What are the benefits? How do you conduct one? How much does it cost? These may be just some of the questions that you may be thinking of right now. We need to start with the fundamental question of just what is a cyber exercise.

As discussed in the introduction, an exercise places the participants in a simulated situation. The goal is to learn from the exercise and be able to use the experiences in future situations that they face.

A cyber exercise performs just that, providing a situation or scenario into which we place the participants to gain experiences and learnings that they can take back and apply. The cyber exercise places your IT security team and, depending on the scope and goals, the IT organization in general in a situation that is cyber security related. Examples include a Denial of Service attack, cleaning up a detected breach, fighting a worm outbreak like Conficker, or any other situation that is relevant within your organization. If you are worried about insider threats, that could be a focus of an exercise. If the corporate concern is how quickly operations can be restored after an intrusion and data breach, an exercise focusing on that will help. If you wish to explore the spearfishing or harpooning (depending on target and definition you wish to use), create an exercise around this and see how the organization handles it. The realms of possibility here are really left to your imagination or your diabolical side, depending on the choices made.

3. Types of Cyber Exercises

3.1. Tabletop Exercises/Paper Exercises

3.1.1. General overview

The goals of a tabletop exercise can vary, but the general principle behind these activities is to step through an event, and examine how the organization is to respond based on policies and procedures. Participants are, as you may be thinking, around a boardroom or conference room table, walking through the event and examining how the activities occur. It is not intended to test the people responding to the event, but rather to help the organization determine whether there are gaps in the procedures, updates required for policies, updates in contact listings or if changes to the organization need to be properly reflected in the corporate documentation.

3.1.2. Requirements to conduct

To conduct a tabletop exercise, the first and most important item needed is the scenario that will drive the exercise. The scenario needs to be carefully planned and thought out to ensure both a realistic situation will be explored as well as a properly defined scope for the overall exercise. A poor scenario will lead to poor exercise results. Luckily there are numerous resources available to help ensure the exercises are planned properly. The Department of Homeland Security has published a guide providing guiding principles for exercise development. (Department of Homeland Security, 2013) The Federal Emergency Management Agency has a course titled *Exercise Design*, Course Number IS 139, which is intended for exercise planners. The course includes an entire section on tabletop exercises to guide the planners through the process. (Federal Emergency

Management Agency, 2014) A third source of guidance is the *National Exercise Good Practice Guide* from the European Union Agency for Network and Information Security within the. (European Union Agency for Network and Information Security, 2009) Each of these sources provides information to assist the scenario planners to help ensure this step is developed correctly.

Another key item that is needed is the organization policies and procedures that are to be utilized within the exercise. While participants may be aware the policies exist, they will not have them memorized. Providing these documents to the participants in a single location will help ensure smooth running of the exercise.

A final item needed to properly conduct this type of exercise is to ensure that the correct participants are chosen and available to take part in the exercise.

3.1.3. Business impacts

The business impacts of a tabletop exercise are minimal, as there is no additional risk the business is being exposed to. The impact is unavailability of personnel during the exercise. Depending on the duration of the tabletop exercise, the absence could be from several hours to several days.

The other main business impact from this type of exercise is the time required to develop and facilitate the exercise. Scenario development, team coordination and report writing all take time to complete, and there must be a prime assigned to perform these tasks. Most organizations do not have a full time resource performing and coordinating exercises, so this will be a secondary duty assigned to someone. This duty, however, is vital to the success of the event. Regular duties for this individual will need to be reassigned, impacting the business.

3.1.4. Business Risk

Similar to the business impact, there is minimal business risk. The largest business risk is again associated with personnel not being available for regular duties during the exercise. This will create a broader exposure for the organization for actual incidents and events, but if the situation is truly serious, the exercise could be interrupted to deal with a developing critical situation.

3.1.5. Benefits and considerations

A tabletop exercise brings a large amount of value to an organization that has not conducted one in the past, or that does not regularly review and update their policies and procedures. By forcing the organization to follow these processes, the organization will identify the problem areas and determine which documentation needs to be rewritten. The exercise will also identify to the organization whether there are process that are missing from the current policy suite. The execution of the procedures will also provide details on where there are gaps in the current policies, procedures and processes. Another benefit of the tabletop exercise is that it is normally a quick item to run. Completing the run through of an exercise, depending on the scope and people involved can take up to a day to do. So holding the exercise doesn't take extensive time from the participants and within most organizations, this can be scheduled with some advanced planning.

A consideration to take into account when planning a tabletop exercise is to schedule it prior to the review and updates of the corporate documentation. This can provide valuable feedback into that process and, if timed correctly, can result in fairly rapid changes to the policy suite documentation.

3.1.6. Drawbacks and considerations

With any exercise, there are folks who will find the exercise type chosen useful and those who will feel they didn't gain much through the process. For the technical staff within your organization, a tabletop exercise will not provide them with the hands-on application of knowledge that is generally desired from training. While there is valuable information gained from the exercise, there are minimal technical skills needed during this process.

The planning and preparation work for a tabletop exercise cannot be overlooked. The exercise is completely based upon the scenario chosen, which is based upon the goals of the exercise. Without proper planning and preparation, the benefits to the organization will be minimal.

3.2. Online or hosted environments (e.g. Netwars)

3.2.1. General overview

Online environments provide for connectivity to a simulated environment where the participants are able to connect, perform the needed actions and then log out, all without impacting the organization's production or other environments. The online environment provides the scenarios for the participants, all infrastructure and computer assets that are needed for interaction during the exercise, and normally provides feedback of what occurred in the exercise and how well the activities were completed.

Hosted environments are fully outsourced and off-site locations that participants travel to (or potentially remotely connect to) in order to conduct the exercise. Generally participants are placed into a classroom setting of some form, and provide the defensive resources to protect the infrastructure provided to them.

An example of an online environment would be SANS' Netwars (SANS, 2014). This offers participants the ability to progress through multiple levels and challenges, and leads to a 5th level where you protect your castle from other participants. Another, more situational focused environment, is the SANS' CyberCity. CyberCity is a scaled model with SCADA components with specific scenarios for the defenders to repel. Some would argue this model would be more realistic, with cameras providing feedback on various aspects of the city and timelines for scenarios to be completed (e.g. train derailment of the next scheduled train forcing a time limit (SANS Institute., 2014)

An example of a hosted environment is the ThreatSPACE Cyber Range, offered by iSIGHT Partners. The environment provides the digital landscape in which participants need to attack or defend targets and work through scenarios. Scoring is provided for the success of the exercise. (iSIGHT Partners, 2014)

3.2.2. Requirements to conduct

To be able to participate in this type of exercise, the organization has minimal items to perform. It needs to procure the services, and it needs to be able to commit the resources to the exercise. For most organizations, this approach to procure periodic services is a huge benefit. There are no additional resources needed within the organization to plan, create, run or schedule the exercise. Staff assignment and time away from the office is all that is needed once procurement is completed.

3.2.3. Business Impacts

The impact on the organization is very minimal. The largest impact is the resources being away from the office or engaged in the exercise and not able to perform their normal duties.

3.2.4. Business Risk

The risk exposure to the organization is also very minimal, but is dependent on which resources are participating in the event. If the IT security staff is permitted to be offsite and not available for regular operations work for a 3 day exercise, there may be a large risk to the organization. The potential impact and risk must be measured against the organizations priorities, security posture and potential for attack to determine the risk. However, this is a manageable risk and able to be contained to the level acceptable to the organization.

3.2.5. Benefits and Considerations

This type of exercise is very rapid to set up and conduct in most cases. In a hosted environment, the exercise is only limited by the availability of staff and the external hosting company's schedule. Accordingly, the online environment can be very quick to set up and commence. For example, the Netwars from SANS can be active within a couple of hours of request and payment for the access. This speed and rapid accessibility provides for access when needed, since the environment is setup and waiting to be used. Another benefit is that scenarios to be used in the exercise are either static and already created by the hosting organization, or at least some have been generated and are available to be used as is or possibly customized. This again saves time and effort on the part of the organization, as planning time and scenario generation work have been completed previously. If there is a scenario available that fits the needs of the organization, it can be quickly chosen and be ready to run through.

3.2.6. Drawbacks and Considerations

The benefits of this exercise type also play into its drawbacks. The ability to have a rapidly accessible exercise is a benefit, but the drawback is that some of these environments have no ability to be tailored to meet even small organizational changes. Netwars has 5 levels, each with questions that need to be answered. While the levels do change periodically, they cannot be tailored to or for the organization. This limitation would be similar for numerous providers. The tradeoff for rapid use is inability to be flexible in the product offered. This needs to be weighed against the needs of the organization. The ability to use these environments provides large returns for their first use, but the benefits diminish with each subsequent use.

3.3. Simulated and virtual environments (virtual systems)

3.3.1. General overview

Virtualization has grown in use for production systems as well as creating lab environments. A use of the technology that would benefit the cyber exercise is the creation of an environment where the cyber exercise can run, but has no impact on the production or other systems in use by the organization. Specifically, creating a virtual production network provides a similar look and feel to the production network, and permits for a “quick reset” if problems arise within the environment. Numerous virtualization technologies are available from VMware, Microsoft and Virtual box, to name but a few.

Simulators are devices or services which provide a virtual environment where you are able to interact with the systems, perform changes and monitor behavior throughout the exercise being run. This is all performed in a setting that, while created to be comparable to a production network, is not a production network. Simulators do have one potential draw back, in that if you have a device simulating the traffic from a large number of systems, you may not be able to directly interact with those systems. It does depend on the simulator and its method for creating the environment.

A simulator is “A machine for simulating certain environmental and other conditions for purposes of training or experimentation” (Rh Value Publishing, 1989). These could be either an internal simulator, where your organization deploys and manages the simulator, or an externally run environment, where you purchase time to perform the exercise. An example of a simulator is the Exata product from Scalable Network Technologies. Information on Exata can be found at http://web.scalable-networks.com/content/exatacyber . Another example of a product that can be used to simulate network activity and events is the Ixia product Breakingpoint. Information on the Breakingpoint product can be found at http://www.ixiacom.com/products/ixia-breakingpoint .

Both simulators and virtual environments offer a faster and cheaper means to create a network to perform numerous tasks, including exercises than building the network traditionally.

3.3.2. Requirements to conduct

The primary requirements to create a virtual or simulation environment are time and money. The need to design and create the architecture requires the time and skills of the correct people within your organization. To then procure the software, hardware and other required components requires, depending on the size, a significant amount of capital. That is on top of the efforts needed to create and run the exercise after the environment is set up.

The exercise needs are similar to most other in-house run exercises. The scenario must be planned and created, the goal defined, and the configuration performed. The expertise to run the exercise is needed, as is the expertise to properly document the exercise both before and after it is complete.

3.3.3. Business impacts

The business impacts, beyond the capital expenditures, are similar to the outsourced /hosted options previously discussed. Resources will need to be assigned to participate in the exercise, and therefore will not be available to take part in the day-to-day operations during the exercise. A benefit to a virtual environment/simulation type of exercise, though, is that if a major incident does occur, the exercise can be placed on hold and resources quickly brought back to the operational network to assist, since they would be within the organizational offices. Suspension of the exercise would be the recourse of last choice, but still a possibility in extreme situations.

3.3.4. Business Risk

Business risks for this exercise type are similar to the hosted solution. The number of staff involved in the exercise may create a situation in which the business is going to be inadequate in its operational capacity. This is a business decision that needs to be made to determine the acceptable risk profile, while still attempting to maximize the knowledge gain from the exercise across as many employees as possible.

3.3.5. Benefits and Considerations

A large benefit to an in-house virtual or simulated cyber exercise platform is the ability to customize and tailor the goals, scenarios and resources available however you wish. The limit here is what is available to the organization to put towards the environment. It could be a five (5) server infrastructure being simulated, or a 10,000 node network. That is one of the benefits of this type of environment; it is quick and easy to turn on new features and functionality, or to create complete new hosts. In a simulator, this can be even easier, as you need to specific what type of host, and the type of traffic you wish to have, and generally the simulator starts to generate the type of traffic you desire.

Virtualized environments offer the ability to halt systems fairly quickly, restore them to a previous state, or to pause their use to name but a few features. This can aid during an exercise that is taking longer than planned, or permit an exercise to be split up over multiple days.

A final consideration is a new type of simulator under development, according to published research, that would be worthwhile to watch and potentially utilize within an organization. A project within Defence Research and Development Canada is developing an automated computer network defence system that offers simulation ability. This simulation would be based on the actual network under observation, and permit the operator to identify the sources of attack and the targets to which the attacker wishes to gain access; the system will provide details on how the attacker can reach this goal. (Defence R&D Canada, 2013) (Sawilla & Wiemer, 2011) This type of simulation, does not appear to be large scale, however, it would provide direct feedback on how the production network could be improved, based on this simulation work, permitting direct application of knowledge and an improved security posture for the organization. It is an interesting concept that may be worthwhile to monitor and investigate further as the research matures.

3.3.6. Drawbacks and considerations

There are several drawbacks from this type of exercise and environment. First, there is a cost to create and maintain. The initial procurement is one cost, but there are also the ongoing maintenance and support costs that also require proper budgeting. Without on-going support, the virtual/simulation environment runs the risk of being set up but left to become obsolete as the technology and software becomes out of date.

Another drawback is that this type of environment will require resources to help keep it current and up-to-date, and even running. Depending on the size of the environment, this could range from a quick sub-duty for an individual to a full-time resource needed. The resource needs must be evaluated prior to deploying the environment, because without proper administration, the environment will become stale, equipment will break or need updating,

The organization, undoubtedly at some point, will suffer an outage, and at some point in an outage, it will be suggested to take a piece of equipment from this environment and swap it for a broken production one, and be replaced at a later time. Be very cautious in this approach, since at some point, something will not be replaced, and then will not be available when needed for an exercise. While the production network will be functioning, this exercise environment does run the risk of becoming the spare parts store with replacements forgotten and reconfiguration widespread.

A final drawback is that, while every effort can be made to create an environment that functions and looks like the production network, the virtual/simulated environment will never be the production network. There will be differences and some resources will point this out as the reason the exercise failed, since the test environment wasn't identical to the organization’s production network. The decision needs to be made regarding how close to the production network this configuration will be.

A final point on this type of environment: If your organization is considering this type of investment, and there is resistance to the capital expenditures, it may be worthwhile to look at creating a preproduction lab environment and gain further usage of the equipment.

3.4. Preproduction testing environments

3.4.1. General overview

A preproduction testing environment is used within most organization as the testing and quality assurance (QA) location where software and hardware are tested by the QA team to ensure that it meets the desired goals, performance and project needs prior to being released to production. It is a risk reduction location, as any problems with new software deployment will hopefully manifest here instead of when deployed to production. To maintain the effectiveness and usefulness of this testing, this environment must be kept as close as possible to the production network, in terms of software and hardware used, patch level and even configurations.

Running a cyber exercise in the preproduction environment will permit organizational resources to utilize similar systems as they use daily in production, while minimizing the impact to the production network.

3.4.2. Requirements to conduct

With this type of environment in place within the organization, the requirements to conduct the cyber exercise are the planning, scenario creation, goals and objectives of the exercise itself. There is also a potential to require some small configuration changes to properly permit the exercise to run.

There will also be the need to back up each of the systems in this environment prior to the start of the exercise, and to restore the configurations to how they were after the exercise. This will ensure that the QA team has systems in a known state, permitting proper testing.

3.4.3. Business Impacts

There are some small impacts to the organization in utilizing the preproduction environment for a cyber exercise. First of all, for the time it takes to prepare, run and return the preproduction environment to its original state, testing and QA activities will need to be suspended. This will impact roll out activities to the production network and has the potential to impact project schedules. The impact can be mitigated by properly planning for the exercise and projects, but the impact will still exist.

3.4.4. Business Risk

The business risk associated with using a preproduction environment is similar to the business impacts mentioned above, relating to the downtime within the QA environment. Project delays for testing and implementation during the exercise may pose a risk to the organization, and an emergency deployment would not be possible to test prior, due to reconfiguration.

To reduce this risk, key business systems may need to have some alternative means to conduct testing should it be needed in an emergency situation. Ensuring the procedures are in place for restoring these key business systems, and testing these processes will reduce the risk.

3.4.5. Benefits and considerations

The benefit to the cyber security exercise is the same as that the reasons an organization create a testing and QA environment: to create a location that closely resembles the production network, while not being the production network. Being able to utilize this environment for a cyber exercise is great. It provides a realistic network in which to work, but minimizes the business impact and risk associated with conducting similar activities on the production network.

3.4.6. Drawbacks and considerations

In selecting a preproduction location in which to perform an exercise, there are minimal drawbacks to the organization. The sole drawback is not the exercise itself, but is related to the preproduction environment and its availability. The main purpose of the environment is to permit testing for production deployments. With the environment being used for an alternative purpose - the exercise - testing will not be possible. However, this drawback can be mitigated and minimized by advanced scheduling of the exercise.

3.5. Penetration Tests

3.5.1. General overview

Core Security defines a Penetration (Pen) test as "a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users' adherence to security policies. " (Core Security, 2014) Having someone attempt to break into your organization can provide an excellent opportunity for training, as you know the when the attacker (the penetration tester) will be attempting to break into the network. A penetration test exercise can be performed in two means: either announced or blind. In an announced exercise, the staff are advised that there is a penetration test occuring, and set the goals for the staff within this exercise. A goal may be to have the system administrators detect the timeframe when a specific system is compromised, or the network intrustion analyst determine there is malicious traffic on the network, to give but two examples. Once the goals have been set, all that is required is to permit individuals to perform their work.

In a blind exercise, goals are still set, but these are not communicatied to staff prior to the event. Staff perform their roles as they normally do, but it is expected that some abnormal behaviour is detected on te network and alarms will be generated. How the participants reacte to these activities is truly interesting to see. Permitting staff to perform their functions within any changes will provide valuable feedback to the organization that may not be discovered during an announced exercise.

3.5.2. Requirements to conduct

In order to conduct either an announced or blind exercise, the prime component is the penetration test. A large number of organizations are under compliance requirements that force the need to have a penetration test perform on their environment yearly, or any time there is a significant infrastructure change. (PCI Security Standards Council, 2014) What this means is that a large number of organizations require little additional items to conduct this type of exercise.

What is needed is to determine what areas on which to focus the exercise. If you wish to test the effectiveness of your intrusion detection equipment, or the adaptability and responsiveness of your intrusion prevention system, those could be two areas on which to focus. Testing the response time to alerts or times to declare an incident could be measured. How the team follows procedures in incident response plan, or how effective the call outs to standby personnel are all valid items to exercise. The world really is your oyster here, as you have a known adversary with known targets and a known timeframe. This permits the organization to focus on areas where it is desired or needed most.

If the organization does not need to regularly perform a penetration test, there is still the opportunity to having the cyber exercise included as an added benefit of the penetration test when submitting the business case.

Planning is required prior to the event, to help determine where the exercise focus will be. There will also be the need for debriefing with the team after the exercise, and reporting to management. However, this commitment is minimal compared to some other types of exercise.

3.5.3. Business impacts

This exercise adds minimal impact to the business on top of the penetration testing being performed. The penetration test itself would have potential business impact, but that is not the focus of this paper. There is some additional overhead for the resources in the organization, as they will be investigation and responding to "false" incidents that the penetration testing company does. Therefore, a real intrusion could slip by unnoticed for a longer period of time than it would have under normal circumstances.

There is also some minimal impact to the team preparing for the exercise, deciding where the focus areas would be. Workload would also increase for the debriefing and report writing. These may be extra duties that require workload adjustment for a short period of time.

A cost impact could be felt by the organization, depending on when call outs happen to the incident management team. If after hours, or additional staff is brought in due to events from the exercise, policy or agreed upon compensation (call out cost) would impact the organization budget.

3.5.4. Business Risk

For a penetration test type of exercise, the business risks are associated with the team's efforts focusing on finding out what is happening as a result of the penetration tester, rather than focusing on real incidents that could be occurring within the organization at the same time, regardless if announced or blind. The risk needs to be examined in the context of the organization to determine if this is significant or not. For example, the impact on a small/medium business in a manufacturing sector would be different than the impact on a small/medium defense contractor, as the threat actors wishing to gain access to those networks would be different and as would the frequency of incidents within the organizations. These considerations should be part of the initial planning and approval cycle to have the risks agreed to.

3.5.5. Benefits and considerations

A penetration testing exercise offers a large number of benefits to the organization for typically minimal costs. Assuming the cost of the penetration test are already accounted for and running that test is agreed to, having an exercise for the team in their "home" setting using the tools and resources normally available allows for a more natural response than some other exercise types. When someone is sitting at their desk doing what they do every day, they are more relaxed and will act how they normally do instead of an off-site activity where they may have the mentality of either "I want to win" or "This is a waste of time."

3.5.6. Drawbacks and considerations

The major drawback with regards to a penetration test exercise is that the work being performed is occurring on the production network. However, this drawback is related to the penetration test itself, rather than the exercise. The risk and impact to the organization would have been agreed upon when the penetration test was authorized.

A second drawback may be that the organization's staff may be aware that a penetration test is happening, and therefore not put the effort into repelling this attack. This will limit the benefit of the exercise if this occurs. Legitimate attacks may also be missed, as they are incorrectly attributed to the penetration test by staff.

A potential drawback to the penetration test is that, due to running the exercise, there may be a delay for the penetration testers, as systems could, for example, be configured to shun traffic or staff could be actively repelling the "attack". This needs to be carefully monitored, and when the impact is too great to the penetration test, the exercise needs to be halted. This will allow the penetration test to complete and fulfill its required goals and objectives.

4. How do you create and run an exercise

While not the main focus of this paper, pointers to several resources that can assist in the creation and running of an exercise are given below.

First of all, running an exercise is not necessarily a complex task. An exercise can be fairly simple or could be a 2 week-long process. It depends on your organization and goals. The more complex the intent and goals, the more likely you will require someone who is dedicated to creating and running the exercise.

There are three main ways that your organization will be able to create and run the exercise. They are as follows: Use in-house people to do it, hire outside resources and expertise to run it for you or fully outsource it. Depending on which type of exercise you are planning, some or all of these options may be possible.

If the choice is to perform the exercise in-house, there are numerous online sources of information that can assist.

One that may assist with creating an exercise can be found through Independent Study Course, IS 139, from FEMA. This free course can be found at http://training.fema.gov/is/courseoverview.aspx?code=IS-139 at the time of this writing, and has the stated goal to "…cover the purpose, characteristics, and requirements of three main types of exercises: Tabletop exercise Functional exercise Full-scale exercise. In addition this course will cover: Exercise evaluation. Exercise enhancements. Designing a functional exercise." (Federal Emergency Management Agency Emergency Management Institute, 2014) It is an excellent source of information for people tasked with creating and running an exercise.

A second source of information is the Department of Homeland Security document "Homeland Security Exercise and Evaluation Program". It can be found at https://www.fema.gov/media-library/assets/documents/32326. This document goal is to "… provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning." (Department of Homeland Security, 2013). While not cyber security focused, the document does provide a framework that can be used for any type of exercise, including cyber related ones.

A third source of information, from the European Union, is the *National Exercise – Good Practice Guide*. It can be found at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide and provides to the reader "a good practice guide to assist authorities in Member States to better understand the complexities of exercises and help them prepare local and national ones" (European Union Agency for Network and Information Security, 2009). The guide was created to help EU member states plan and run exercises, and provides guidance directed to people with little experience in running those exercises. It is also cyber security focused.

If the desire is to hire outside expertise to run the exercise, then it is critical to ensure that those outside resources have run exercises of the type and size the organization is looking at. Ensure that numerous references are provided and follow up with those references to determine if the skills needed within your organization exist. The same should be considered when outsourcing the entire exercise. The extra steps here would be to ensure that the outsourcing company has the resources available to run the exercise following the planning stage, either directly or through their partnerships.

5. Conclusion

Exercises play an important role in many organizations' readiness today. The Federal Aviation Administration, most military organizations, and numerous emergency responders participate in exercises regularly. These are conducted to help evaluate if the procedures, equipment and training in place are effective and successful in meeting the needs of the organization. Exercises themselves also provide training and learning opportunities for the participants, as some may not have had to deal with the situation the exercise is delivering.

Most cyber security operations teams are very similar in their roles in the IT department as emergency first responders are in the general public. When something is going wrong or doesn't seem right within the IT organization, the cyber security team is normally called to assist. The teams' alarms, notifications and investigations need to be conducted quickly, effectively and seamlessly on a day-to-day basis. To assist in preparing the teams to meet the challenges of their roles, cyber exercises can play an important role within an organization.

Exercises expose team members to realistic situations in which they can draw upon their knowledge, skills, equipment and training to resolve. By providing the environment and opportunities for the organization to perform exercises regularly, there will be benefits to the organization. These benefits include increased awareness of cyber security, improved preparation of staff to handle complex situations confidently, and augmented skills of the security team. These also lead to an improved security posture of the organization. Regular cyber security exercises should form part of every organization's operational plans.

6. Appendix – Summary comparative table

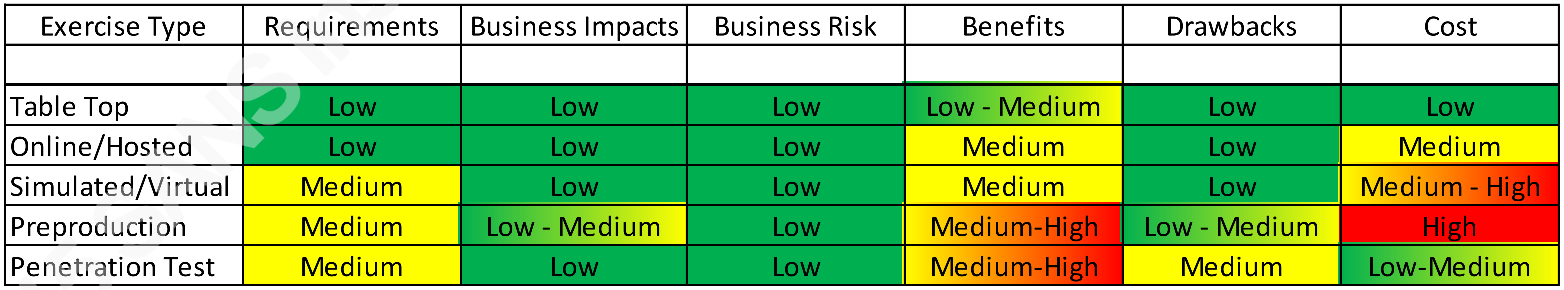
Below is a summary table containing a brief overview of each exercise type, and a categorization for each of the discussed areas

Low is colored Green

Medium is colored Yellow

High is colored Red

Blending occurred when it was between two levels, such as low-medium, it blends from green to yellow.



Exercise Type	Requirements	Business Impacts	Business Risk	Benefits	Drawbacks	Cost
Table Top	Low	Low	Low	Low - Medium	Low	Low
Online/Hosted	Low	Low	Low	Medium	Low	Medium
Simulated/Virtual	Medium	Low	Low	Medium	Low	Medium - High
Preproduction	Medium	Low - Medium	Low	Medium-High	Low - Medium	High
Penetration Test	Medium	Low	Low	Medium-High	Medium	Low-Medium

References

ANC R&D. (2014). *Cyber Exercise Planner*. Retrieved December 29, 2014, from Clearance Jobs: https://www.clearancejobs.com/jobs/1846133/cyber-exercise-planner

Augustine, T., & Dodge Jr, R. C. (2006). Cyber defense exercise: meeting learning objectives thru competition. *10th Colloquium for Information Systems Security Education*, 61-67.

Branlat, M., Morison, A., & Woods, D. (2011). Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise. *Human Systems Integration Symposium*, 10-25.

Carr, S. A. (2014, October 2). *Cyber: The new Red Flag battleground*. Retrieved December 29, 2014, from US Air Force: http://www.af.mil/News/ArticleDisplay/tabid/223/Article/503204/cyber-the-new-red-flag-battleground.aspx

Core Security. (2014). *Penetration Testing Overview*. Retrieved December 29, 2014, from Core Security: http://www.coresecurity.com/penetration-testing-overview

Cotman, C. W., Berchtold, N. C., & Christie, L.-A. (2007). Exercise builds brain health: key roles of growth factor cascades and inflammation. *Trends in neurosciences, 30*(9), 464-472.

Davis , J., & Magrath, S. (2013). *A Survey of Cyber Ranges and Testbeds, DSTO-GD-0771*. Defence Science and Technology Organisation, Cyber and Electronic Warfare Division. Sydney: Defence Science and Technology Organisation.

Defence R&D Canada. (2013). *ARCHIVED ARMOUR TDP Automated Network Defence*. Retrieved December 29, 2014, from Government of Canada, Public Works and Government Services Canada: https://buyandsell.gc.ca/cds/public/2013/05/29/3698551d82c73be475d852f0decffb4f/ABES.PROD.BK__SV.B051.E25450.EBSU000.PDF

Department of Homeland Security. (2013, April). *Homeland Security Exercise and Evaluation Program*. Retrieved December 17, 2014, from Federal Emergency

Management Agency: https://www.fema.gov/media-library/assets/documents/32326

European Union Agency for Network and Information Security. (2009, december 17). *National Exercise - Good Practice Guide*. Retrieved December 29, 2013, from European Union Agency for Network and Information Security: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide

European Union Agency for Network and Information Security. (2012, October 25). *National and International Cyber Security Exercises: Survey, Analysis & Recommendations* . Retrieved December 29, 2014, from European Union Agency for Network and Information Security: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012

Federal Emergency Management Agency. (2014). *IS-139: Unit 1 Exercise Design*. Retrieved December 29, 2014, from Federal Emergency Management Agency: https://training.fema.gov/emiweb/downloads/is139unit1.doc

Federal Emergency Management Agency. (2014). *Unit 5: The Tabletop Exercise*. Retrieved December 29, 2014, from Federal Emergency Management Agency: https://training.fema.gov/emiweb/downloads/is139unit5.doc

Federal Emergency Management Agency Emergency Management Institute. (2014). *IS-139 Course Materials*. Retrieved December 29, 2014, from FEMA Emergency Management Institute: http://training.fema.gov/is/coursematerials.aspx?code=is-139

Harris, K. (2014, December 18). *Marines exercise crisis response training before deploying*. Retrieved December 29, 2014, from WCTI12 Channel 12 news: http://www.wcti12.com/news/marines-exercise-crisis-response-training-before-deploying/30304002

iSIGHT Partners. (2014). *ThreatSPACE Cyber Range* . Retrieved December 29, 2014, from iSIGHT Partners: http://www.isightpartners.com/products/threatspace/

LohrMann, D. (2014, July 27). *A new cyber exercise: Test your security team's incident response capabilities*. Retrieved December 29, 2014, from Government Technology: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/A-new-cyber-exercise-Test-your-security-teams-incident-response-capabilities.html

Merriam-Webster. (2014). *Dictionary*. Retrieved December 29, 2014, from Merriam-Webster Dictionary: http://www.merriam-webster.com/dictionary/exercise

NATO. (2014, November 14). *Largest ever NATO cyber defence exercise gets underway*. Retrieved December 17, 2014, from NATO: http://www.nato.int/cps/en/natohq/news_114902.htm

Paffenbarger Jr, R. S., Blair, S. N., Lee, I.-M., & Hyde, R. T. (1993). Measurement of physical activity to assess health effects in free-living populations. *Medicine and science in sports and exercise, 25*(1), 60-70.

PCI Security Standards Council. (2014). *Information Supplement:Requirement 11.3 Penetration Testing*. Retrieved December 29, 2014, from PCI Security Standards Council: https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Penedo, F. J., & Dahn, J. R. (2005, March). Exercise and well-being: a review of mental and physical health benefits associated with physical activity. *Current opinion in psychiatry, 18*(2), 189-193.

Rh Value Publishing. (1989). *Webster's Encyclopedic Unabridged Dictionary of the English Language*. New York: Portland House.

SANS. (2014). *Netwars*. Retrieved December 29, 2014, from SANS Institute: http://www.sans.org/netwars

SANS Institute. (2014). *SANS Cybercity*. Retrieved December 29, 2014, from SANS: http://www.sans.org/course/cybercity-hands-on-kinetic-cyber-range-exercise

Sawilla, R. E., & Wiemer, D. J. (2011). Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework. *2011 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 167-172). IEEE.

Skripnichuk, A. (2014, December 4). *Soldiers prepare for live-fire exercise*. Retrieved December 29, 2014, from Fort Hood Sentinel: http://www.forthoodsentinel.com/story.php?id=14814

United States Government Accountability Office. (2008). *CRITICAL INFRASTRUCTURE PROTECTION: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise*. Washington: United States Government Accountability Office.

University of Hawaii Manoa. (2014). *Poʻoihe 2014 Cyber Security Exercise*. Retrieved December 29, 2014, from University of Hawaii: http://www.hawaii.edu/cyberrange/

Last Updated: June 25th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Singapore 2018	**Singapore, SG**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANS Charlotte 2018	**Charlotte, NCUS**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DCUS**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Cyber Defence Bangalore 2018	**Bangalore, IN**	**Jul 16, 2018 - Jul 28, 2018**	**Live Event**
SANS Pen Test Berlin 2018	**Berlin, DE**	**Jul 23, 2018 - Jul 28, 2018**	**Live Event**
SANS Riyadh July 2018	**Riyadh, SA**	**Jul 28, 2018 - Aug 02, 2018**	**Live Event**
Security Operations Summit & Training 2018	**New Orleans, LAUS**	**Jul 30, 2018 - Aug 06, 2018**	**Live Event**
SANS Pittsburgh 2018	**Pittsburgh, PAUS**	**Jul 30, 2018 - Aug 04, 2018**	**Live Event**
SANS August Sydney 2018	**Sydney, AU**	**Aug 06, 2018 - Aug 25, 2018**	**Live Event**
SANS Hyderabad 2018	**Hyderabad, IN**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS San Antonio 2018	**San Antonio, TXUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Boston Summer 2018	**Boston, MAUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
Security Awareness Summit & Training 2018	**Charleston, SCUS**	**Aug 06, 2018 - Aug 15, 2018**	**Live Event**
SANS New York City Summer 2018	**New York City, NYUS**	**Aug 13, 2018 - Aug 18, 2018**	**Live Event**
SANS Northern Virginia- Alexandria 2018	**Alexandria, VAUS**	**Aug 13, 2018 - Aug 18, 2018**	**Live Event**
SANS Virginia Beach 2018	**Virginia Beach, VAUS**	**Aug 20, 2018 - Aug 31, 2018**	**Live Event**
SANS Krakow 2018	**Krakow, PL**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
Data Breach Summit & Training 2018	**New York City, NYUS**	**Aug 20, 2018 - Aug 27, 2018**	**Live Event**
SANS Chicago 2018	**Chicago, ILUS**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
SANS Prague 2018	**Prague, CZ**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
SANS San Francisco Summer 2018	**San Francisco, CAUS**	**Aug 26, 2018 - Aug 31, 2018**	**Live Event**
SANS Copenhagen August 2018	**Copenhagen, DK**	**Aug 27, 2018 - Sep 01, 2018**	**Live Event**
SANS SEC504 @ Bangalore 2018	**Bangalore, IN**	**Aug 27, 2018 - Sep 01, 2018**	**Live Event**
SANS Tokyo Autumn 2018	**Tokyo, JP**	**Sep 03, 2018 - Sep 15, 2018**	**Live Event**
SANS Wellington 2018	**Wellington, NZ**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Amsterdam September 2018	**Amsterdam, NL**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Tampa-Clearwater 2018	**Tampa, FLUS**	**Sep 04, 2018 - Sep 09, 2018**	**Live Event**
SANS MGT516 Beta One 2018	**Arlington, VAUS**	**Sep 04, 2018 - Sep 08, 2018**	**Live Event**
Threat Hunting & Incident Response Summit & Training 2018	**New Orleans, LAUS**	**Sep 06, 2018 - Sep 13, 2018**	**Live Event**
SANS Baltimore Fall 2018	**Baltimore, MDUS**	**Sep 08, 2018 - Sep 15, 2018**	**Live Event**
SANS Alaska Summit & Training 2018	**Anchorage, AKUS**	**Sep 10, 2018 - Sep 15, 2018**	**Live Event**
SANS Munich September 2018	**Munich, DE**	**Sep 16, 2018 - Sep 22, 2018**	**Live Event**
SANS London July 2018	**OnlineGB**	**Jul 02, 2018 - Jul 07, 2018**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**