



Corporate Cyber Exercises

Are all the certifications and technology worth the money?

Your organization has spent **tens of thousands of dollars** on information security. You've invested in people, process and technology. You have certified personnel, well written policies, and the latest in technology. **Are you sure it all works? Will you be protected?**

In other words; was it worth all the money you've spent, is the new guy on the team as functional as the one with all the certifications, does the new technology truly support your policies, and can all the parts inter-operate while managing a crisis. How do you continue to refine your incident response without going through a live incident? The answer to these questions is simple; A Cyber Exercise.

What is a Cyber Exercise?

A Cyber Exercise is a live network attack against a replica of your system. During the attack you are charged with the same duties and responsibilities within the course and scope of your job function and policies.

The Infrastructure is Real

We work with you to replicate pieces of your technology infrastructure; routers, firewalls, operating systems, applications, etc. An exercise is most meaningful when you train on the same environment that you are charged with protecting.

The Attacks are Real

This is not a penetration test. Any and all attacks are allowed at any time. Since the exercise network is *not* on the Internet, production data and systems are not at risk.

The Policies are Real

Participants in an Exercise are to bring their own operating policies and procedures. This allows them to find out what works under pressure.

The Results are Real

At the end of an exercise you will know the strengths and weaknesses of your people, processes, policies and technology.

But we are already compliant

That may be true. You may be under any number of regulatory compliance obligations (e.g. GLBA, SOX, HIPAA) and feel that you have certified and tested your people, processes, policies and technology. However, each of those items is a



piece; a piece of a greater system that only comes together during an incident. And during a live incident is the worst time to find out that all your certified pieces cannot function under stress.

So how does a Cyber Exercise Work?

There are four steps to conducting a Cyber Exercise; Planning, Building, Execution, and Review and Evaluation.

Planning

During the Planning Phase we work with you to identify the scope of the exercise. We identify key people through job descriptions, certifications, training and experience. We review standard operating procedures, policies and other written documents. We sample deployed technologies and infrastructure. All of this is included in establishing your Exercise.

Building

We take the information gathered during the Planning Phase and build an infrastructure that replicates the necessary pieces of your network. We generate normal office message traffic to create realism. The message traffic is also used to cause your staff to perform functions that they would normally have to do. Rules are crafted to reflect your personnel job descriptions, policies and procedures.

Execution

This is the actual exercise. During this Phase a professional team of hackers attack your network in pursuit of specified objectives. Your team must maintain the confidentiality, integrity and availability of the business process and the systems that support it.

Review and Evaluation

Upon completion of the exercise we conduct a formal review of your performance and give you the opportunity to interact and question the hackers. Scores are distributed to the individual, the team and the business process.

The Benefits

Verify the Fitness Level of your Organization

Protecting your organization's information assets and managing an incident requires several complex systems working together towards a common goal. This 'system of systems' is not unlike the human body where several systems work in concert to support the entire system. In the physical realm we use the work fitness to denote various level of proficiency across the different systems. For example, we look at the health of the individual systems to describe the fitness of the whole. Strength, stamina and flexibility are just some of the ways you can rate your fitness. The same metrics apply to your organization's team.



A Cyber Exercise verifies your organization's fitness level

- Strength – what are your best skills?
- Stamina – how long can you stay in the game?
- Flexibility – how many different types of incidents can the team handle?

Shine the Light on your Security Spending

All those certifications, policies, and technologies cost money. By running your team and infrastructure through a cyber exercise you will be able to identify how well they perform.

External Non-Biased Evaluation

White Wolf Security does not sell or install security solutions. As a result we offer an honest evaluation of the fitness of your people, process and technology.

Scoring and Benchmarking

Over time, as more and more teams roll through their cyber exercises we will be able to provide referential scores and benchmarks. For example:

- How do teams with similar infrastructures perform?
- How do people with similar certifications, training and experience perform?
- How do organizations with similar budgets perform?

Totality of the Review?

Our team of experienced personnel has conducted formal reviews of exercises and even live combat missions. We apply the same critical review of your performance during a cyber exercise.

Next Steps

Like annual visits to a doctor, regular cyber exercises test the fitness of your people, process and technology as things grow and change over time. The more exercises you conduct the more relevant and accurate the metrics are.

Schedule one Today

To schedule a Cyber Exercise or to learn more, please contact Tim Rosenberg or Joe DeCree at 717-295-6201.