



RED CELL **(Penetration Tests & Aggressive Vulnerability Tests)**

Red Cell was a once covert program utilized by the US Navy S.E.A.L.s to test US Military Base security measures and Anti-Terrorism preparedness. Private industry has turned from just “paper whipping” contingency plans to applying the aggressive testing practices of the military’s elite forces to analyze the best planned polices and procedures to see where vulnerabilities still lie and to make immediate corrective actions to strengthen their over all security posture. If you have something to protect it might be worth knowing how well it is protected?

Most IT Departments focus on protecting their network, servers, and IT infrastructure from viruses. What about their physical security program and what about cyber-terrorism or a malicious hacker – say a disgruntled or former employee or even an unhappy customer?

Most IT Departments will tell you they are prepared. How prepared are they? This is the question we at Foremost Response raise for CEOs, Presidents, Vice Presidents, Board Members, and other Senior Executives who know how devastating a successful attack upon their corporate or company infrastructure could be for their business.

What if ...

A disgruntled employee gained access to your servers and network and then destroyed those assets either physically or with a homemade explosive device? How much would it cost you while your network was down? How quickly could you repair the damages?

What if ...

A disappointed customer hacked into your network? How secure are your records? How secure is your vendor information, your client information, and your inventory information? What damage could be done to your business from the outside – are you reasonably protected? What if all they did was alert the media that they had gained access and penetrated your computer network – how would this affect your business?

What if ...

An unethical competitor or independent source wanted your proprietary information? Do you have a program that covers all the bases necessary to protect it – from a physical security standpoint to a secure network? How damaging would

RED CELL **(Penetration Tests & Aggressive Vulnerability Tests)**

it be if that information was accessed/leaked/published/sold – could you recover or would you be devastated?

All of these are questions we ask. Why... because we are in the business of testing your protocols, programs, and procedures against unfriendly attacks.

Without malicious intent, Foremost Response, Inc. assumes the “bad guy” and we hack, expose, and exploit all your weaknesses and discover your worst nightmares before they become realities. We will document and articulate exactly what we have done and how we accomplished our “bad guy” mission of gaining access to what you most wanted protected. Foremost Response Subject Matter Experts then help you fill in the security gaps and develop a stronger more complete protocol to protect those areas and things most dear to your business’s survival.

The Process:

We set up a confidential meeting to discuss your industry and your primary concerns – what do you most want protected and what is most damaging to you if it is lost. Are your fears focused internally or externally?

If Foremost Response accepts the assignment we assemble our team of Subject Matter Experts from our associates and we together analyze your current security posture and we start to identify weaknesses. Then to test our theories we will act on those suspected security gaps as if we did have malicious intent and we would exploit every possible opportunity to gain what you most fear losing... only we will not cause you devastation and we give back what we find.

Who is at Risk:

No industry, no business can fully expect to be safe and impervious to such an event or an attack. Even a natural disaster that was not prepared for properly can bring a business to their knees. If the warning signs were there, if the possibility existed and the proper measures were not implemented will your insurance company still settle your claim? Insurance companies have taken massive blows in this decade and they are likely to scrutinize every claim closely – will you pass that test? Foremost Response works with you to document that you have taken all the reasonable measures, that you have implemented strong protocols, and that you have minimized your risks the best that you can.

Businesses that have taken advantage of Penetration Testing:

Military Installations	Dept. of Motor Vehicles
State & Local Governments	Public Utility Companies
Hospitals & Clinics	Schools, Colleges, & Universities

RED CELL **(Penetration Tests & Aggressive Vulnerability Tests)**

Lawyers & Law Firms	Jewelry Stores
Museums & Art Dealers	Banks & Credit Unions
Software Firms	Property Mgmt Companies
Car Manufacturers	Technology & Computer Manufacturers
Casinos & Hotels	Chemical Manufacturers & Distributors
Ware Housing Facilities	Transportation Companies
Commercial & Private Airports	Ports & Docks
Private Properties & Homes	Post Offices
Pharmaceutical Manufacturers & Distributors	
Oil & Petroleum Manufacturers & Distributors... Pipelines	

Call Foremost Response and let us start taking a look at the worst case scenario for you today before it becomes a reality.

The Challenge:

If we *can not* hack, expose, or exploit anything and your current security program survives the assault; our services are **FREE**.

However, if Foremost Response can hack, expose, or exploit your security program then *all our time is billable*. Foremost Response then will help you fix the security gaps identified and establish or create a stronger security program customized to your needs using the latest technologies and practices.