THE SHIELD GROUP, LLC

Cyber Breach Mitigation Services
Programs, Planning, Training and Response

Regardless of the size of your business, data breaches, ransomware compromises and Advanced Persistent Threat (APT) attacks continue to increase and the odds are at some point your organization will become either an opportunistic victim or the focus of a targeted attack. Business leaders know it is not a matter of "IF" their technology systems and information assets will be targeted, it is more a question of when it will occur, and will they be prepared when it happens. When that day occurs, ask yourself: Will you have a Plan?

While an attacker only needs to succeed once, Security Defenses are expected to protect organizations against 100% of all attacks and never allow an attacker inside – *NEVER* – This is an Unrealistic Goal.

Today's reality is that no company is immune from a possible data breach. No matter how well prepared you are, a breach will quickly uncover the vulnerabilities in your defenses and your response plan. Companies should use the lessons learned from other major organizations who have been victimized, such as Target, Home Depot, Sony, Anthem and Experian. These lessons, from top Fortune organizations, demonstrate how no company is immune from a cyber-attack or data breach, and illustrate the value in having sound preventative measures in place to help identify and alert that an attack may be occurring, and having in place sufficient barriers ("speed bumps") in order to slow the attackers down to thwart data exfiltration. This is critical in order to allow time for the organization to activate their Breach Mitigation and Incident Response Program in order to try to contain the attack.

www.shieldgroup.org
877-480-5529

4470 W. Sunset Blvd.
Office 9-2795
Los Angeles, CA 90027

11700 Preston Road
Suite 660-443
Dallas, TX 75230

18968 Goldwater Road
Suite 100
Westfield, IN 46062

700 12th St. N.W.
Suite 700-6584
Washington, DC 20005

Just having a plan is not enough. Like fire drills, you must practice your plan regularly. Once a cyber-attack happens it is too late to map out your plan or make changes. More importantly, your plan has to be the right plan. It must be multi-faceted, flexible and adaptable, fit your organization and work for you. Borrowing an Incident Response Plan from another organization won't work. That plan was their plan – you need Your Plan.

Without an existing plan, it is nearly impossible to contain or stop a breach, while at the same time conducting the investigation, and also restoring IT services.

Data beach preparedness is a team sport, not a compliance exercise. Your breach response plan:

- Has to involve all the right departments and team members, but still remain nimble to be effective.
- Must be sufficiently broad in scope and scenario planning and contain detailed, yet flexible playbooks that are adaptable.
- Must be extensively and regularly exercised by all members of the team.

Unfortunately, data breaches are not a new phenomenon and will continue to happen.

As an organization you need to be prepared – *In Advance* – With a multi-faceted Breach Mitigation and Incident Response Plan.

If you have questions about your ability to respond to a breach situation or need assistance improving your breach mitigation programs, contact us. We will gladly talk about our experience dealing with some of the largest breach incidents in recent years, and how we helped executive leadership navigate through these challenges with regulators, investigators and clients.

Send us an email using the Contact Form on our Web Site or call us at 877-480-5529.