THE GEORGETOWNGROUP™
STATE OF THE ART INTELLIGENCE

The Georgetown Group is a comprehensive security services firm. Our mission is to protect our clients from fraud and mitigate risk. We accomplish this by providing strategic intelligence and support in order to preempt the multitude of attacks that are common in today's global economic environment. We minimize threats and effectively address them by combining cutting-edge technological resources, a wealth of legal and law enforcement experience, and an international network of trusted sources. The Georgetown Group has been retained by Fortune 500 corporations, public relations firms, law firms, non-profit groups, and individuals.

The Georgetown Group provides a unique service package. Our expertise offers a well rounded, proven team of executives capable of fully understanding and addressing all aspects of our clients' security needs from the ground up. We understand how your business works, where it is vulnerable, and how to eliminate those vulnerabilities.

The world today presents challenges that require innovative strategies and effective solutions. The threat to critical infrastructure and critical intellectual property from cyber terrorism and espionage is at an unprecedented level. Best business practices require an examination of cyber security vulnerabilities. The Georgetown Group provides a straightforward, strategic approach to securing your most important assets from both internal and external threats.

Cyber Security

> *"Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies."*
> *~ White House Cyberspace Policy Review*

Our Philosophy:

The Internet grew from a network of researchers to a global nervous system because practically anyone could access it from anywhere in the world. The Internet has brought about a golden age of communication; information sharing and virtual communication has occurred between cultures that may have never crossed paths. It made a very large world very small. But the Internet is not a safe environment. It is a frontier. The Poneman Institute recently found that the mean annual cost of cybercrime in 2012 was $8.9 million per company and companies experience an average of 1.8 cyber attacks per week. According to US Investigators, China has stolen terabytes of sensitive data – from usernames and passwords for State Department computers to designs for multi-billion dollar weapons systems – from a variety of United States companies, agencies and individuals. The threat is not only external. In a recent study, 60% of employees admitted to taking data of one sort or another from their employers.

At The Georgetown Group we understand that a critical component of any successful business is connectivity and collaborative access to networks. We also know that our clients have information that others desire to gain through unscrupulous and illegal methods. The Georgetown Group offers a comprehensive cyber security management structure that relies on detailed analysis and understanding of your network and information control practices, a review of intellectual property and information protection policies, computer forensics and information

The Georgetown Group
T: 202-656-9950 | www.georgetowngroup.com
E: eoneill@georgetowngroup.com

systems monitoring. We work with you to develop a customized incident response strategy that addresses not only the external hacking and social engineering risks, but addresses internal vulnerabilities from the disgruntled employee to a spy in your organization. Following our philosophy of hand-crafted client service, we recommend practical solutions to protect the flow of information across your organization, while mitigating cost and avoiding adding overly complicated processes to your business practices.

Our Approach:

> *"What is at stake is not just government secrets, but also the safety and security of our infrastructure, the intellectual property that underpins our future prosperity, and the commercially sensitive information that is the lifeblood of our companies and corporations."*
> *~ MI5 Director General Jonathan Evans*

When your data is at risk, the hidden attack can cripple an organization. At the Georgetown Group, we employ an alliance of information security experts, engineers, cyber sleuths and risk control experts to ensure that your system infrastructure is built to withstand threats without causing excessive uproars or create a constant state of crisis. We understand how to defend your systems by being proactive and installing solutions to secure your sensitive information before your enemies discover your vulnerabilities.

Our cyber security services go beyond retroactively securing and proactively building networks. The Georgetown Group employs a holistic approach to cyber security that includes training our client's managers and employees in basic security precepts that can often mean the difference between catching a hacker or spy and loosing critical sensitive information to a competitor.

In conducting our cyber security assessments and implementation we examine four main areas of concern:

I. Analysis of Sensitive Information Control Practices

The Georgetown Group understands that every organization and person has a different level of cyber security need. Accordingly, practices and policies to protect intellectual property and sensitive information will differ. When performing a cyber security vulnerability assessment, our cyber team collects information related to your reporting structure, access to information policies, network resources, and practices to protect the integrity of your data. We then work with our client to hand-craft policies and procedures that fit the specific needs of the organization and defend against threats.

II. Cyber Vulnerability Study

Most companies store their sensitive information and intellectual property electronically. The failure to install sufficient controls to mitigate threats and prevent loss of data will result in cyber theft. Our cyber security team uses state of the art techniques, software and proprietary technology to analyze network and information protection control vulnerabilities, discover data

The Georgetown Group
T: 202-656-9950 | www.georgetowngroup.com
E: eoneill@georgetowngroup.com

security risks, identify whether compartmentalization of critical information is sufficient, and spot potential internal and external sources of attack. Some areas we might examine include: network security, physical security, Web application analysis, enterprise IT risk assessment, and a review of the wireless security structure.

III. Penetration Testing

One of the most efficient methods of discovering vulnerabilities is to simulate an attack on the network and organization in order to discover security deficiencies. During a penetration test, our security experts will seek to gain access to your sensitive information utilizing a variety of methodologies including, social engineering (pretexting, tricking and phishing) attempts, network intrusions, and other typical and proprietary cyber attacks. A penetration test provides you the confidence to know that weaknesses in your network defenses, both electronic and social, are discovered and corrected by our team before your enemies exploit them.

IV. Cyber Security Implementation Plan

Once we know your vulnerabilities, and have fully tested your system to simulate an attack, the Georgetown Group works closely with you to provide a detailed report on our findings, with practical and actionable recommendations for mitigating vulnerabilities.

V. Cyber Security Training and Policy Implementation

The Georgetown Group will train your personnel to manage the cyber security system we build for you. We work with your executive team to draft or revise policies that control and protect sensitive information. We also hold training sessions for your employees and managers, either in person or web-based to educate your organization on cyber penetrations and provide practical advice to discover weaknesses and attacks, report them timely and proactively, and help prevent the loss of critical information.

The Georgetown Group
T: 202-656-9950 | www.georgetowngroup.com
E: eoneill@georgetowngroup.com