ECI®

CYBER SECURITY & INTELLIGENCE

Cyber Security Services for Today and Tomorrow

Every day, hackers exploit online vulnerabilities to access potentially sensitive government agency and business information. The most commonly known intrusions are via spam, malware including viruses, worms, and Trojans, as well as phishing attacks and insider threats. In addition to this list, we wish to emphasize the concern for Advanced Persistent Threats (APTs). APTs are more carefully propagated to access certain targets, for example with the goal of obtaining secrets or R&D of private sector high tech industries. This white paper highlights the increasing demands on businesses and government agencies alike, to protect their information. Furthermore, this paper explores what we all must do to successfully protect that information.

Cyber Security is a multi-tier effort. We need to mitigate threats by *preventing* cyber security threats, by *detecting* current and potential threats, and finally, by *responding* quickly and efficiently to cyber attacks. Due to the vast number of threats faced daily, businesses and government agencies alike need to work together, as a cohesive team, to protect our information and fight cyber intrusions and attacks.

We hope you find this white paper useful and welcome your feedback and constructive ideas on what else you believe ECI-LLC, businesses, and the industry in general, should be doing to ensure Cyber Security.

Increasing Demand for Cyber Security Service

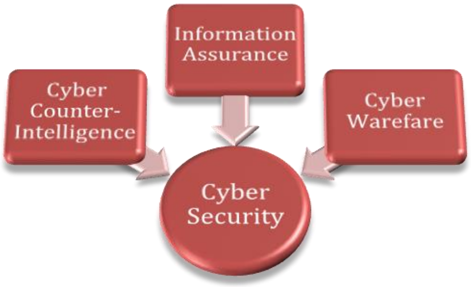
In the last decade, there has been a rapid increase in cyber intrusions and attacks, leaving us vulnerable to the exposure of sensitive information, the disruption of operations, and to an increase in operating costs. Billions of dollars have been spent and budgeted for cyber security, not only to combat these attacks, but also to prevent, detect, and respond to the on-going threats we face every day.

- On April 7th, 2009, The Pentagon announced they spent more than $100 million in the last six months responding to and repairing damage from cyber attacks and other computer network problems.
- On April 1st, 2009, U.S. lawmakers pushed for the appointment of a White House cyber security "czar" to dramatically escalate U.S. defenses against cyber attacks, crafting proposals that would, for the first time, empower the government to set and enforce security standards for private industry.
- On February 9th, 2009, the White House announced that it would conduct a review of the nation's cyber security to ensure that the Federal government of the United States cyber security initiatives are appropriately integrated, resourced, and coordinated with the United States Congress and the private sector.
- In the wake of the cyberwar of 2007 waged against Estonia, NATO established the Cooperative Cyber Defense Centre of Excellence (CCD CoE) in Tallinn, Estonia, in order to enhance the organization's cyber defense capability. The center was formally established on May 14th, 2008, and it received full accreditation by NATO and attained the status of International Military Organization on October 28th, 2008. Since Estonia has led international efforts to fight cybercrime, the United States Federal Bureau of Investigation said it would permanently base a computer crime expert in Estonia in 2009 to help fight international threats against computer systems.
- One of the hardest issues in cyber counterintelligence is the problem of *attribution*. Unlike conventional warfare, figuring out who is behind an attack can be very difficult. However, Defense Secretary Leon Panetta has claimed that the United States has the capability to trace attacks back to their sources and hold the attackers "accountable."
- The total 2014 budget for DOD cyber security projects has been increased to $5.1 billion, and U.S. Cyber Command (USCYBERCOM) will add 4,000 new personnel to its ranks by 2016.

ERROR: couldn't open
ERROR: unable to
ERROR: couldn't read
ERROR: unable to write to
malicious virus; Install;
Boot sector was successfully
bindery

Cyber Security: Areas of Defense

It is worth repeating that Cyber Security is a multi-tier effort: we need to mitigate threats by preventing, detecting, and responding to cyber attacks. However, before we can prevent, detect and respond, we must first understand the different areas of cyber security that must be addressed. These areas are: *Cyber Counter Intelligence*, *Cyber Warfare*, and *Information Assurance*.



Cyber Counter Intelligence

Cyber counter-intelligence encompasses measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well encompassing foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

Cyber Warfare

Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare, although this analogy is controversial for both its accuracy and its political motivation.

U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), defines *cyberwarfare* as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.” The *Economist* describes *cyberspace* as “the fifth domain of warfare,” and William J. Lynn, U.S. Deputy Secretary of Defense, states that “as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . which has become just as critical to military operations as land, sea, air, and space.”

Information Assurance

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation, and confidentiality of user data. It uses physical, technical, and administrative controls to accomplish these tasks. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. These protections apply to data in transit, both in physical and electronic forms, as well as data at rest in various types of physical and electronic storage facilities. Information assurance as a field has grown from the practice of information security.

The Solution: Working Together

Due to the vast number of threats faced daily, businesses and government agencies alike need to work together, as a cohesive team, to protect our information and fight cyber intrusions and attacks. Government Agencies have already begun addressing the needs by introducing more cyber security policies and platforms, in addition to dramatically increasing cyber security budgets. Now, businesses must do their part to ensure cyber security.

Eddy Challita International (ECI) LLC takes this responsibility seriously. ECI, a Small Business company established in 2001, specializes in Cyber Security solutions. ECI’s professional and up-to-date staff members are ready to tackle any challenge that comes their way. To effectively mitigate Cyber Security threats, ECI offers risk analysis and technical services to ensure your organization is protected. ECI offers these solution services to federal and state governments, the Department of Defense, and other federal and private sectors.

ECI Cyber Security professionals provide proactive defensive/offensive solutions, by ensuring all elements of modern and up-to-date Cyber Security protocols, best practices, and tools are used effectively. ECI’s team holds various certifications in Cyber Security, among them: CEH, CISSP, Security+, and Encase Forensics. These are some of the examples of the training that ECI’s 8570-compliant staff will bring to your organization, to help secure your networks.

“We know the cyber field; we know intelligence; and we know how to exceed customer expectations. We are ready to start helping you now.”

-*Edward Challita, ECI-LLC President and CEO*

ECI-LLC
8160 Maple Lawn Blvd
Suite 200, Fulton,
Maryland, 20759