SypSec®
Security Solutions

Security Controls Assessment Options

Strategies to Defend Offensively

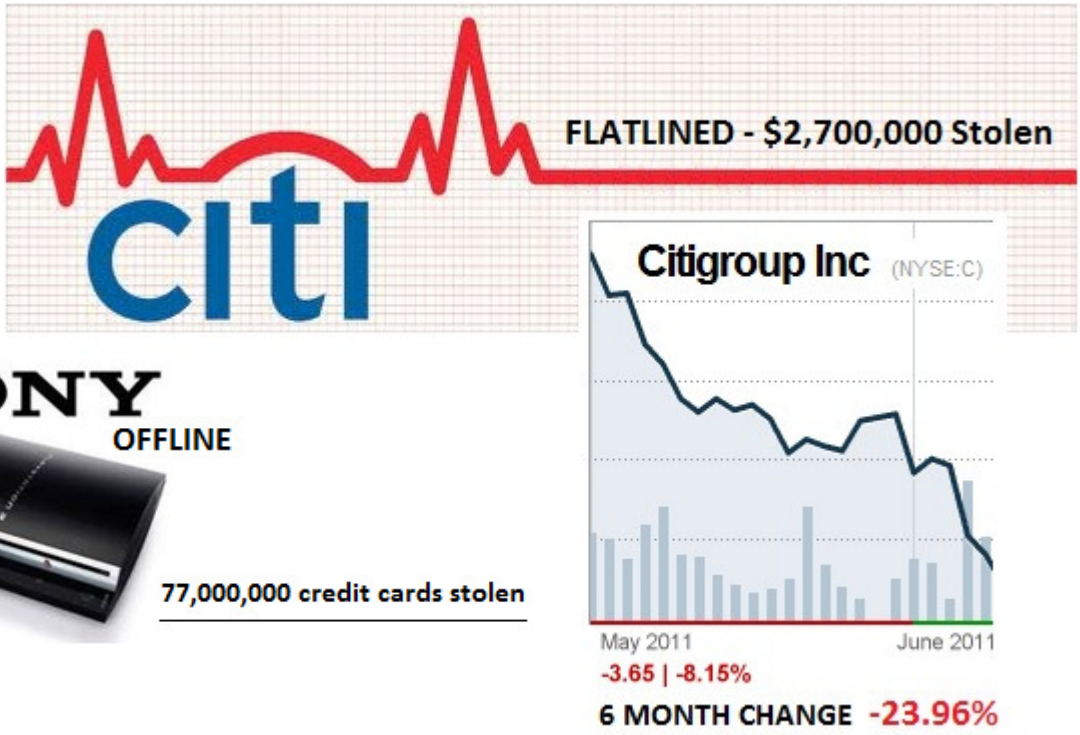
By George Sypsomos

SypSec®
Security Solutions

INTRODUCTION

With the recent increase in global media attention to the antics of hacker groups such as "Anonymous" and "Lulz", the threat to information assets has evolved to the forefront of many organizations' considerations when contemplating the value of allocating funds for Information Assurance (IA) investments. The threat of damage to an organization's reputation is a serious consideration for stakeholders, as is the threat of losing corporate or government secrets to competitors and enemies.

Consider the damage inflicted upon Sony, the US Central Intelligence Agency, Citigroup, The US Senate, and Booz Allen Hamilton… Perform a Google search on "Lulz incidents" – nearly 2 million search results.



So you think you are safe because you are not in the news? Consider this quote from PricewaterhouseCoopers' forensic department director Kim Peretti:

> "There are probably some corporations and credit cards that haven't been hacked."

Peretti has stated that there **MIGHT** BE a few entities which HAVE **NOT** BEEN hacked. The entities which have not been compromised are more than likely limited to valueless targets; although, even these seemingly valueless targets (e.g. home computers) can be used as part of a massive attack known as a Distributed Denial of Service (DDOS) attack. Home users also often use their home computers to tend to their banking and online bill payment processing needs. The gravity of Peretti's statement cannot be ignored.

STRATEGY

What can you do about it? Simply turning on the local Windows firewall, turning on automatic updates, and installing an antivirus solution are NOT going to suffice for organizations serious about protecting their assets. A more comprehensive approach is necessary. Many organizations do not have the resources to entertain the process of building their own IA programs, and many do not have a large enough organization to justify investing resources in the creation of their own program.

Enter a security-focused Independent Verification and Validation (IV&V) team, which can review your management, operational, and technical security controls in a custom-tailored process, scaled to your organization's specific needs. SypSec will meet with your stakeholders to determine the best assessment plan for your organization, carry out the assessment within scope, and deliver after-action reports and recommendations which you can use to protect your assets. The assessment can be small and focused or large and comprehensive.

Our initial interviews and questionnaires will determine whether a Basic or Advanced Security Controls Assessment would be recommended for your organization.

Basic Assessment	Advanced Assessment
Requirements and scope determination	Requirements and scope determination
Develop Rules of Engagement	Develop Rules of Engagement
Perform Testing	Perform Testing
Generate Report	Generate Report
Provide General Recommendations	Provide General Recommendations
	Provide Remediation Procedures
	Develop Plan of Actions and Milestones
	Perform Follow-Up Testing

The Security Controls Assessments are broken into three tiers with varying levels of comprehensiveness. The levels of comprehensiveness are depicted in the following matrix:

	Tier 1: Penetration Testing	**Tier 2:** Internal Vulnerability Scanning	**Tier 3:** Cyber Security Assessment
Thoroughness	**Low** (Assesses perimeter defenses and DMZ accessibility, can also include intelligence-based attacks such as phishing)	**Medium** (Internal asset scanning, can also scan DMZ from external source or internal networks)	**High** (Comprehensive assessment including policy review, configuration review, scanning, requirements analysis, etc.)
Cost	**Low to Medium**	**Medium**	**High**
Resulting Recommendations	Manual – detailed and specific, require +time to prepare	Automated from COTS or Manual from custom scanning	Manual – detailed and specific, require +time to prepare
Preparation Time	**Short**	**Short**	**Long**
Completion Time	**Medium**	**Short**	**Long**
Note: The generalizations *short, long, and medium* are used to discern each from one another, not to quantitatively measure any given amount.			

PROCEDURES

Requirements and Scope Determination

In order to ensure that your investment in an Information Assurance review provides the most value, SypSec Analysts will provide a pre-assessment questionnaire prior to scheduling the assessment, which will allow them to prepare a comprehensive assessment platform. We will also meet with your IT/IA personnel and management stakeholders to review the regulatory requirements and scope of the assessment to ensure that the assessment is comprehensive.

We will not waste our clients' resources with tests that do not benefit their organizations. If you have already determined whether you need a Basic or an Advanced assessment and have already determined the tier of testing you would like completed, the process of Requirements and Scope Determination will be as simple as checking boxes for what you need to be tested.

Develop Rules of Engagement

Prior to performing an assessment, our personnel will develop a set of guidelines to be followed during security testing, based on the requirements and scope that have been previously determined. This is known as the Rules of Engagement (ROE), and is intended to remove scope creep from your assessment, to protect your assets from unintentional damage, and to keep you informed of any severe threats as they are discovered during the test procedures.

Testing

Once a plan of action has been determined, our personnel will custom-tailor their testing platform with the necessary tools to complete your assessment in accordance with the requested scope, and then coordinate with your organization on completing the test procedures.

Reporting

After the test procedures have been completed, our analysis team will review the test data and analyze the level of threat presented by the findings in the data. We will develop and deliver a report detailing the findings, and will provide recommendations and specific technical remediation procedures (Advanced Assessment), which your organization can undertake to improve the security posture protecting your assets.

Continuous Monitoring

As part of our Advanced Assessment, we will provide a Plan of Actions and Milestones (POA&M) which lists the weaknesses discovered and the milestones involved in correcting them, suggests time lines for completion, identifies relevant regulatory controls, suggests recommended responsible personnel resource types, and appends notes such as general mitigation and remediation suggestions. Our team will also follow-up with your organization's IA personnel, and will be available to answer questions regarding the delivered products. We will also perform validation testing to ensure that the specific findings from your assessment have been remediated - *test, correct, validate*.

RECOMMENDATION

SypSec Solutions can provide many options to define the inherent weaknesses in the security posture of an organization. We recommend a full-scope Cyber Security Assessment of all three security controls areas – Management, Operational, and Technical – combined with the implementation of a continuous monitoring program to ensure that your organization's assets are protected now, and are continued to be protected in the future. With each successive assessment during the continuous monitoring program, the latest vulnerabilities will be addressed to ensure that exploitation by threat entities will only be possible through zero-day weaknesses or through social engineering efforts. SypSec Solutions can also test for unknown vulnerabilities, and can test for user awareness to social engineering, but that is a story for another white paper.

Make The First Move…