

## Topic: ICAC – Cyber Security Threat Assessment

AzoogAds, Inc.

Contact Person: Michael Sprouse, CMO, [msprouse@azads.com](mailto:msprouse@azads.com), (212) 308-8509 x3297, [www.azoogleads.com](http://www.azoogleads.com)

Date: 10/10/07

When one looks at the components of computer crime it's revealed to be the same as any other crime. There's an attacker and a victim, and the attacker requires the same three components to be successful - **Motive, Opportunity and Means (MOM)**.

Looking at IT security history, the bad guys were always far more sophisticated than the people who tried to stop them. Even if companies or the government could conceive of IT security it was almost impossible to achieve it because of the lack of knowledgeable security professionals out there and the lack of security protection tools in the marketplace.

Today, MOM is more powerful than ever. Even a novice can download powerful intrusion tools and can find free written guides to penetrating systems. **The motive is there because there is no barrier to entry for an attacker.** Millions of pages of free instruction are available to anyone interested in reading it - **massively accessible Means**. In a few minutes you can hack a bank account and steal someone's life savings because there are still many financial institutions that are not protecting their clients and their systems with any sophistication - for some this presents **irresistible Opportunity!** So we see the stage is set today - powerful Motive, perfect Opportunity and the best Means.

The **vulnerability** in the electronic space **can be reduced**. There are many products and strategies that can be deployed. There are many robust tools that log attacks and prevent them in real-time. These tools and strategies can provide security for a committed company or government organization. As long as the **defense is treated as an ongoing process** that is constantly updated and **not an end-state**, the battle can be well-waged.

More and more computer crimes are being sent to court and attackers are being sent to prison. This is good and needs to continue. Computer crime needs to be prosecuted just like physical crime so that when attackers try to attack a virtual target they will have the same chances to be caught and punished as criminals committing crimes in the physical world.

Can we conclude that if companies or our government applies their focus and attention to providing ongoing modern IT security then most of the attackers can be easily kept unemployed? Unfortunately we cannot. As attackers are blocked from attacking one way they will seek another. Attackers previously attacked **networks and hosts** until it became too difficult so they switched their focus to attacking **applications** which were more vulnerable than hosts. Being blocked at the application level now, **attackers are preying on the end users directly**. This can easily bypass most company's IT security protocols and processes. In the last few years we see new attack patterns like **XSS, Phishing and other client side attacks** which take advantage of the fact that most individual users know nothing about IT security or their role in keeping things secure.

It was noted above that a bank with weak protection could be compromised in a few minutes. A bank where IT security is current and advanced, can be much more difficult to compromise through a direct system attack. A **much easier way** to attack a bank account in a protected institution would be **to trick a user into providing all of their login and access details**. This is the goal of most Phishing emails we see on a daily basis. These emails often ask for some sort of verification - in fact most of these emails are dressed up as security checks! In reality **the user is redirected to a cloned website where the login data is captured and later used to compromise the account**. Shockingly the best way to get someone's security details such as a login ID and password combination is to just ask them for it!

Root causes of ongoing security threats are **older operating systems** at home (most users are still running Windows 95/98), **no anti-virus protection**, and the general view of the computer as a home appliance. Unlike a refrigerator which might run 10 or even 20 years, a computer cannot be used for the same length of time. **We need to help increase security education and awareness** and to encourage people to form new habits while breaking old ones (e.g. stop writing passwords on post-its and sticking them to the monitor). The more the country knows the more we can protect ourselves from the bad guys and we must invest in marketing this education and it needs to be a high priority item on the government's agenda.