



Cyber Intelligence Protection And Containment Services

"CYPACS"

Who's monitoring and protecting your company brand and reputation online?

If you're like most companies, you have little or no clue what confidential information or comments are being posted and discussed on the Internet both publicly or in black hat areas. With the addition of social media sites like Twitter, Facebook, LinkedIn and others there is now even a larger cyber-world for individuals to share and distribute information about your company and brand. Of course, some of this information will be true and confidential while other information is purely false and aimed at damaging your company and brand. How important is your brand and reputation?

Would it be important to know any of the following?

- People are talking about successfully hacking into your systems
- People are slandering your company, brand, or reputation online
- Someone is preparing to take legal action against your firm
- Confidential company data is being posted to the Internet
- Disgruntled employee is slandering your company and employees online
- Employees are illegally downloading "restricted" data to thumb drives
- Employees are sharing passwords or confidential data among themselves

If you can say "**Yes**" to any of the above you need to learn more about **CYPACS**.

Here's a brief overview:

CYPACS service is unique among other types of Intelligence gathering and anti-phishing solutions. The CYPACS methodology includes a total protection and a risk containment model to the already well established uses for proactive information gathering. Using information resources obtained over thirty years in the security arena **CYPACS** can gather information about potential events that may impact business functions or your customers such as:

- Threats against key vendor sites that could compromise your data integrity or availability.
- Discussions of Physical security weaknesses as it may also impact logical security.
- Online technical discussions or confidential data leakage either by your employees or ex-employees.
- Underground chat channels, hacker boards and other sources that may have information about current hacks, attempting exploitation or current attempts and successes.
- Statements related to the privacy, confidentiality or security of customer account information.

The CYPACS service goes beyond delivering the above items. It also has the experience and knowledge to discern real threats from idle talk. IPAC has a proven reputation for detecting exploits and remediate those threats on customers systems. Also by applying previous knowledge to the information gathered the CYPACS property risk model gives you a real world assessment of that threat, be it from a supposed leak in your SQL servers, to discussion of exploits in you external websites.

The CYPACS service also provides intelligence about phishing and Web site hijacking with a twist. Other services monitor for chatter or postings about a phishing e-mail or have exposed systems to capture mass e-mail that may contain references to your company. **CYPACS** does that as well, but CYPACS analysts' also proactively scan for trends in exploits, social engineering or compromises that fit in your industry profile. CYPACS then delivers a risk profile that let's you know what risk impact your company may have to similar issues.

And CYPACS analysts' deliver the one thing that is most important beyond the information intelligence gathered; that is the expertise to remediate, contain and eliminate the treat, be that from a technology threat such as a cross site scripting vulnerability in your website to "take down" of the "copy cat" website or e-mail phishing site.

Don't Wait Until It's Too Late!