

All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Information Sharing – The end of security?

I recently completed a report (shameless plug) as a principal consulting analyst for Tech Vision Research (www.techvisionresearch.com) on the future of information sharing. I won't be detailing the 40 pages or so here, but I do want to summarize some of my thoughts.

Sharing seems inevitable

It appears that sharing is no longer optional or preventable. It is a fundamental of the information age and a necessity for success in any endeavor involving people. Rather than seeking to restrict it, for the vast majority of cases and information, the greater benefit comes from finding better ways to share desirable information with more of the target audience.

Attempts to suppress sharing, even in the extreme, lead to catastrophic failure. If you don't believe me, look at Manning, Snowden, Clinton, and Putin. Encryption schemes are essentially all of limited lifespan, except perhaps the perfect system, which has as much key material as content and depends on being able to securely distribute the keys, which is done physically. Even then the endpoints are the vulnerabilities, and humans sit there.

It's about your focus of attention

The tension between sharing and restriction of information has existed since the beginning of human history. In the information age, that tension has become so stark and obvious, that it must be addressed by individuals and organizations of all sorts. From "information needs to be free" to the highest level of trade secret and classified information controls, regardless of perspective, the issues are in dire need of being addressed.

In some notions of theory, shared knowledge is far more efficient and effective than isolated pockets, while in other notions of theory, information has more content and utility when it is more rare. In practice, and according to Mayfield's paradox,¹ it is almost impossible to have a valuable secret so protected that almost nobody knows it, and yet it is also almost impossible to have information known by everyone.

As a result, the only realistic thing that can be done is to (1) find the things you really need to share, and share them as well as you can, (2) find the things you really need to not share, and try hard to protect them realizing you will ultimately fail, and (3) provide support for users to share more safely for everything else, help them understand why its important to be safe, and make it easy to get their job done so they don't have to bypass the system to do so.

Conclusion

Get over it. Information sharing is almost always more of a benefit than a deficit. Stop imagining that secrecy is the heart of cybersecurity, because it is not. Integrity, availability, use control, accountability, custody, and transparency are usually more important. Help people share effectively while assuring these other properties and we will all be better off. Want more details? See the shameless plug above...

¹ Mayfield; Cvitanic (2000). "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security". Information Systems Control Journal 2. Retrieved 2010-07-12