Herding Cats:
Using the Popular Press

October 2009

BrandenWilliams
SECURE BUSINESS GROWTH

The popular press is kind of like a squirrel—always searching for nuggets yet lacking attention span. If you saw *Up* this summer, think of Dug. Find the biggest story to one up my competition and get the exclusive to—SQUIRREL!

Longtime professionals know that security is a long-term process. There is no security light switch to toggle—it cannot be done overnight. In fact, unless a major overhaul in the culture and attitude toward information security occurs, companies tend to revert back to their pre-breach lifestyle. I've witnessed a laser focus on security blur to a beam you might find emanating from that flashlight you keep for emergencies, but never seem to remember to change the batteries; weak, unfocused, and not painful to shine directly in—SQUIRREL!

The popular press[1] needs negativity. They need it so badly that good news stories are derided and called *fluff* pieces. Real news must have a bad guy or bad event behind it. The treatment of information security in the popular press mimics this same attitude. Don't expect Brian Williams to talk about how great we're doing securing data because we've been breach free for many months.

The press has been involved in security for a long time, but not always reporting breaches. If you were alive during World War II (or if you paid attention during history class), you might remember phrases like "Loose Lips Might Sink Ships," "Defense On The Sea Begins On The Shore," and "Defense In The Field Begins In The Factory." If this was not the first time that the country organized an information security movement on a large scale, it certainly was one of the most significant. These slogans were designed to remind people that any information about troop movement can give the enemy valuable information to mount an attack. While these slogans were created by the U.S. Government, they were widely reported in the media.

The media reports mostly on breaches or big security violations or scandals today. Usually for the popular press to get involved, something bad either has already happened (like when dealing with a breach), or is about to happen (like when dealing with a virus or trojan horse). In either case, the popular press can be quite useful!

The popular press aims to incite action in individuals when discussing events that are about to happen. Confickr created quite a stir this year, and the media helped get the word out. Larger businesses generally have staff to assist with impending threats, and in most cases they do a really good job at preventing major impact to the business. Small businesses typically do not.

Imagine yourself finally quitting the rat race to start a photography business. You have a $20,000 investment to make in your business, and you know at least one computer is going to be part of that. Modern photographers use computers to edit their work, create value added offerings like DVDs, enable online ordering systems, and manage finances. What they don't typically do is add extra security to their networks, encrypt their sensitive files, and monitor the overall security posture of these systems. Users without constant support will suffer the most from security events on the horizon. The media helps to get the word out, inciting them to act.

FOOTNOTES

[1] For the purposes of this article, the term "popular press" does not include information security related publications.

When the media reports on events that have already happened, it provides useful information about the breach, legal and financial ramifications of the breach, what consumers can do to get assistance if their information is stolen, and makes examples out of the breached and the attackers (if they are caught)[2]. Information security is a relatively young science, and has only dealt with mass adoption in the private sector after companies connect themselves to the Internet (again, in many cases). This information is tremendously useful to small and large businesses alike when reviewing their risk management process and to learn vicariously though another company's mistakes.

The challenge with the media is dealing with the--SQUIRREL--problem and discovering and managing the influx of information in a reliable manner. Remember, not all experts are ACTUALLY experts, and in this business, people are quick to offer their opinion on the facts especially if they don't know the facts (because the ones that do are typically bound by confidentiality agreements).

Use the popular press as one of the many tools in your arsenal to defend against hackers.

FOOTNOTES

[2] The TJX Companies breach is a fantastic example of this. There is almost too much information to digest on their breach.

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.