NEW HAVEN REGISTER
http://www.nhregister.com/columns/article/Forum-Asleep-at-the-switch-why-so-many-sites-11376685.php

Forum: Asleep at the switch: why so many sites get hacked

By Bill Murray **Published 3:31 pm, Wednesday, December 17, 2014**

Sony has been hacked several times. Its latest embarrassment is directed at itself and is just one more example of the lack of security on the internet. You might just wonder why that can be. Everyone knows the internet is plagued by viruses and malware. Hackers have stolen millions of credit card numbers and set them for sale, thus making the entire banking industry plan to change the very card you use. It must be obvious that something is going on to someone.

Almost everyone at this point across the United States has a firewall installed at their home and business. It's the little box you use to get to the internet. It may also provide the wifi you use, the one with the blinking lights. At corporate locations and at the home offices, routers are installed there as well. Many of the more expensive models include features not included in the small consumer ones. Are they the same you might ask? Home units are not even close to the real ones. The ability to monitor what is going on is the main drawback to most of the home-based units.

The difference between firewalls is broad; it can be explained, however, like security in a building. Many buildings have locks and video surveillance. Some have security guards sitting at the entrance keeping people away that don't belong there. Some have elaborate systems with magnetic locks and everyone must wear identification inside the building or office.

Unattended firewalls act primarily as a guardian for inbound communication. That is why virus and malware activity has grown so significantly over the last decade. Some reports suggest that between 82,000 and 127,000 new malware programs are released daily. Unchecked, these applications can give total control over a network or any computer or device that is attached to it. This makes it possible for the computer or device to do anything it is instructed to do on the inside of the firewall.

Attended or monitored firewalls can spot suspicious outbound traffic and act accordingly. Target Corp. had a data breach in December 2013. It ignored its warning system for which it spent over $1.6 million and allowed one of the largest losses of

credit card numbers in history. That is not to say that every loss involves such a grievous error. In the recent losses at **Home Depot**, reports have been made that management ignored warnings that the company was vulnerable to attack. It is not really a surprise for some of these companies to lose information.

Many retail systems at malls and big box stores have physical network connections unprotected. Many of the same organizations also have back-end wifi connections that can also be compromised.

The only guarantee is that unchecked systems will continue to lose information. What would make a difference in the lackadaisical attitude toward security would be a looming threat of legal action against companies who lose information. It would also require that the courts put more emphasis on the burden that individuals face when their information is lost. A couple of years of credit monitoring often is typical compensation for an ensuing a lifetime of trouble faced by the millions affected.

On more than one occasion I have heard people say they don't care about internet security, yet they lock their cars and their homes. Your connection to the internet is made to the entire world. There are far more people on the internet that can do harm than in anyone's neighborhood.

Bill Murray of West Hartford is a forensic computer technician. Under the pen name Trip Elix, he is author of books including “Extortionware: A Hackers Tale," the forthcoming title “A Right To Property;" he blogs at **http://tripelix.com**.