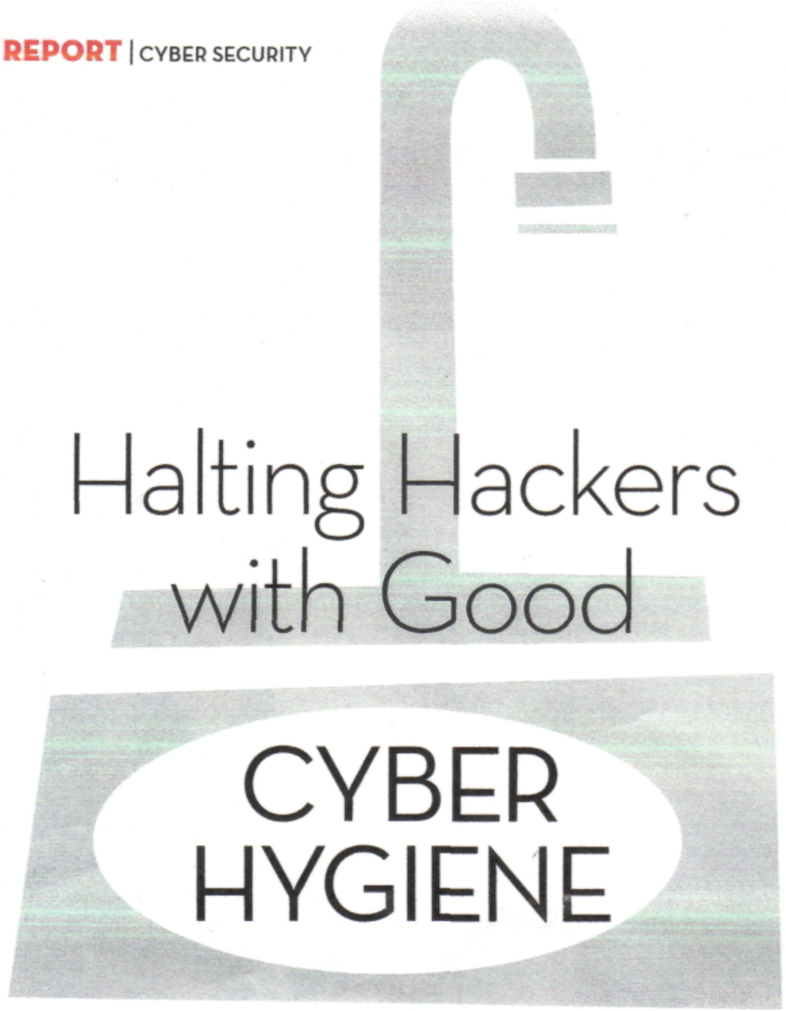


Halting Hackers with Good CYBER HYGIENE

Millions of computers are under a constant, multi-level and multi-faceted attack designed to steal information. But nearly 80 percent of cyber crime can be prevented.

BY KRISTI M. ROGERS

SECURITY AND RISK EXPERT; VICE CHAIRMAN AND FOUNDING CEO, AEGIS LLC.

It's an attack that you cannot see, but you most certainly have felt it. According to government figures, the United States has lost hundreds of billions of dollars as the result of cyber crime, cyber espionage and cyber war. In today's economy, one would think that the alarm bells would be ringing. It's happening now, it happened yesterday, and it will happen at an even greater extent tomorrow.

The National Security Administration's director general, Keith Alexander, states that economic espionage through cyber attacks is the "greatest transfer of wealth in [American] history." It does seem a bit unreal. Unfortunately, it is very real. Most security experts today will tell you that there are only two types of companies in the United States: one that knows it has been "hacked" or attacked via its computers, and the other that does not know it has been attacked.

- In 2011, software company Norton estimated U.S. costs due to cybercrime at $140 billion, $32 billion of which came directly from theft, the rest as a result of time lost to repairs from malware. ($388 billion in worldwide costs)
- Growing threat: the Ponemon Institute's sample grc saw a 50 percent cost increase to companies fr cybercrime and a 40 percent increase in the frequency attacks from 2010 to 2011

Even if your identity has not been stol your computer may have been co-opt to serve in a vast net, a "zombie army" tl disrupts, attacks and steals on a large scale. W are the attackers? Is it the teenager in his her parent's basement with bunny slippers a a Mountain Dew who has just hacked into t

AN URGENT PRIORITY

What to watch on the Hill

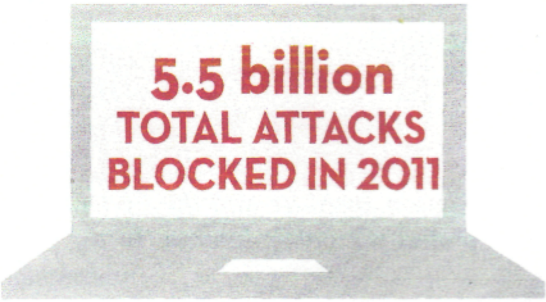
Cyber security for U.S. companies, the government and citizens is complex. Recent reports about attacks on organizations such as Sony, Lockheed Martin and PBS seem to surprise many, but this is not a new phenomenon. They relentlessly pursue secrets and intellectual property at a mind-blowing pace; and this is very different from the pursuit of financial gain that drives cybercrime.

Some members of Congress are addressing this growing threat to protect our personal finances, our jobs and our economy. "From my end," political strategist Rachel Pearson of Pearson and Associates notes, "the human side of the very productive working relationship between Republican Rep. Mike Rogers (chairman of the House Intelligence Committee) and Democrat Rep. Charles Albert 'Dutch' Ruppersberger is central." Together, they recently sponsored the 13-page "Cyber Information Sharing & Protection Act (CISPA)" bill, described as a "critical and necessary first step" that passed th House with overwhelming bipartisa and industry support.

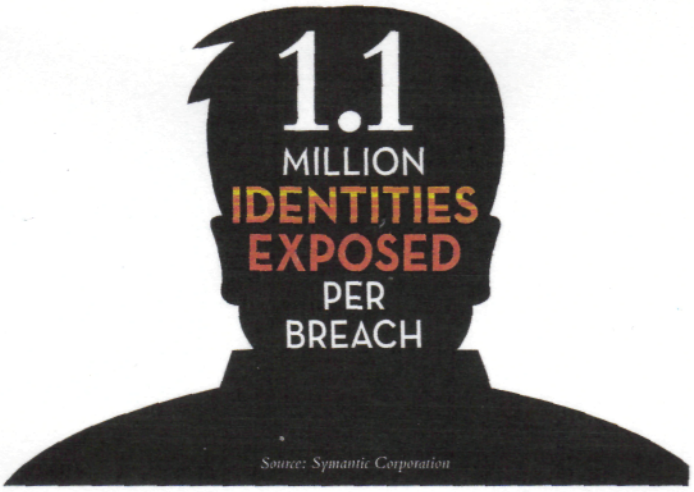
WHAT CAN YOU DO TO PROTECT YOURSELF?

Tips to secure your personal computer and prevent cyber crime:

- Update operating systems and software to the latest versions to protect yourself from "malware" - malicious software that can be installed on your machine without your knowledge.
- Even emails from people you know may contain malware links or attachments if an account has been hacked; be careful when following links and visit websites by entering the addresses directly into your browser.
- Encrypt sensitive, personal data.
- Change passwords regularly.
- Do not provide personal information on social networking sites such as address or birthday.
- Do not log into personal accounts over public WIFI networks.
- Do not plug unknown USB devices into your computer.



Source: Symantic Corporation



Source: Symantic Corporation

principal's computer to change his grades? We should all wish for those days. Today, the attackers are lone "entrepreneurs," organized "hacktivists," and cyber crime syndicates — organized syndicates, mercenary for sale, nation state warfare, zombie armies, invisible botnets, Operation Shady Rat — this sounds like the trailer for the next movie blockbuster, or the next Vince Flynn novel, or even the next Avengers movie. Unfortunately, this is today's reality.

> "EVERY YEAR, AN AMOUNT OF INTELLECTUAL PROPERTY LARGER THAN THAT CONTAINED IN THE LIBRARY OF CONGRESS IS STOLEN FROM NETWORKS MAINTAINED BY U.S. BUSINESSES, UNIVERSITIES AND GOVERNMENT DEPARTMENTS AND AGENCIES." — *Department of Defense*

Sony President and CEO Howard Stringer

A few examples highlighting public cases of cyber attacks:

SONY CORPORATION: One of the most newsworthy attacks in recent history is that of Sony. In 2011, hackers breached Sony's customer network compromising more than 70 million records. Sony estimated the cost at $171 million.

STRATEGIC FORECASTING: A data breach at the intelligence analytics firm, Strategic Forecasting, disclosed in December 2011, was attributed to Antisec, a "hacktivist" group affiliated with Anonymous that used the 68,000 stolen credit card numbers to make donations to charity.

EPSILON: The Texas-based marketing firm suffered a data breach in 2011 in which 60 million names and email addresses were stolen from customers for more than 50 major retailers and banks. Estimate for the total costs — projected to include forensic analysis, monitoring, fines, litigation and lost business reputation damage — var from $100 million to as much as $4 billion.

TJ MAXX: In 2007, the clothing retaile breach caused by a remote intrusion resulte in the compromise of more than 94 millio credit card accounts, estimated at $64 millio in costs. WL