The Quiet Threat to Industry and America

America's New National Security Issue

A serious epidemic of data loss is encroaching upon industry and business in the United States.

How serious is it?

FBI: "Business models have been compromised and critical innovation pipelines have been hijacked. Our economy and national security are under relentless attack. Economic security is America's "new" national security issue." https://summit.fbi.gov/about.html

The FBI held a special invitation only summit across the US at FBI offices and invited experts and companies offering solutions. In early July I was invited to attend the FBI National Intellectual Property Protection Summit on 15 September. I attended the summit with FBI agents at a secure aerospace contractor facility.

This article serves as part of my responsibility to help educate industry and the business community as outlined by the summit. Before the summit began I obtained a Criminal Justice Information System (CJIS) certificate to be able to

view and work with sensitive classified data. Attendees were warned not to record the event and that some identifying information was considered restricted. The FBI Director, James Comey, greeted us and the summit ran for 3 hours with experts from across the US discussing IP loss and what business and industry can do to stop it. Speaker Bios can be found here.

Why did the FBI get involved and hold the summit? Business in the USA as a whole is not very healthy. According to the FBI we have been in cyber war since 2005 with attacking countries increasing transgressions on an exponential basis. Due to the increasing rate of data theft, the US cannot sustain a healthy economy for very long without our economic security being undermined. How much Intellectual Property is being lost?

According to the FBI, https://summit.fbi.gov , in 2014:

- $600 Billion is the impact of intellectual property breaches on the global economy.
- $300 Billion of intellectual property breaches occur in the US alone!
- $6 Trillion is the calculated worth of intellectual property in the United States.
- 40 Million is the number of American jobs vulnerable to intellectual property theft.

$300 Billion was lost within the US in 2014 according to the summit dialog and 2015 is outpacing last year. The numbers are realistically on the low side for several reasons. Data loss is underreported by companies both public and private because:

1. The news hits the bottom line quickly
2. Losing data undermines confidence
3. It is embarrassing
4. It is a new problem - Industry is unprepared and is reactive instead of proactive.

Let's bring this home a little. Most of our readers are in the engineering, petrochemical business and related services. Attendees viewed a map of the US indicating major losses in millions of dollars to industry represented by a red dot

for each loss. The entire eastern seaboard from the Mid-Atlantic States upward to Cape Cod was solid red. Naturally, I looked at my home in Florida and saw significant losses. Then I shifted my attention to my second home state of Texas having lived there three times. My eyes centered on Beaumont, Texas with 5 huge losses in 2014 totaling over $1.2 billion. The names of the corporations are restricted but everyone would recognize them. Houston, Texas was solid red like the northeastern US. I didn't have time to total those even larger losses there for last year.

Recently the DoD defense contractor Leidos was awarded a $4.3 billion contract for data cyber security. This award size is unprecedented for data security and serves as an indicator of magnitude of data loss in the US. That contract is announced here

How are losses calculated? Of those companies that report data loss the FBI sends in a team on a confidential basis to ascertain all aspects of the breach and to work with accounting personnel to make estimates and projections to what the data theft costs the company.

Who is stealing data? You have a good idea if you watch the news regularly because you can't miss the almost daily data loss reports. The primary offenders are China, Russia Military, Russia Industrial Espionage (organized crime), and North Korea. However, attacks are coming from a myriad of countries in Eastern Europe, the Middle East and Africa – so it seems everyone is getting into cybercrime, because it is a shortcut to profit.

Why are these countries and other criminals stealing IP data? This is a big question and I won't pretend to know the entire answer. However, the motives of many attacks are clear; to hurt us economically and as a possible prelude to future aggression. This is one reason why the US government is requiring more data handling security from contractors performing their work. In the future, if you intend to do government work you will have to prove the working data is secured.

Setting this issue aside let's look at another obvious reason for data theft. Thieves want to learn what you and your company knows. They want to bypass what it costs your corporation in time and money to obtain your intellectual property and

operating knowledge. Stealing data, IP and the secrets of operating a business simply helps criminals start a business without the same costs.

FBI summary: "The tactics employed by bad actors are continually evolving, but their basic approach remains somewhat static: steal valuable intellectual property (IP), skip the costly R&D stage, systematically degrade their competitor's business model, and then diminish their market share and the value of their research with predatory and/or destructive practices. The global marketplace features several nations relying on economic espionage as an integral part of their country's business model." - https://summit.fbi.gov/about.html

China, for example, is notorious at stealing company information. With the knowledge of how to start and run a business a cheaper labor source can undercut the heretofore competitive prices and thus steal market share.

Examine the far reaching economic damage of IP theft. Take an example of war; when a country bombs a factory to put it out of business to disrupt production. Eventually the factory is rebuilt, some workers are replaced and production resumes. When intellectual property and operating knowledge is stolen to set up a competing business at lower costs the "factory" or US business is displaced in the market and is shut down. The factory does not reopen, workers lose their jobs, they do not have money to spend and the tax base is reduced. Thus begins an economic decay in trickledown effect through our economy.

Simply examine the repeating history of what happens to countries with a weak or collapsing economy. If a country loses economic viability it is done. This is equally true of corporations on a smaller scale within US industry. Now you understand the awful and insidious scenario that the FBI wants to prevent by educating Government, Industry and Business to stop data loss.

What can you do? First, be proactive instead of reactive. Second, recognize it is a real and growing problem. Educate yourself how Data and IP Loss happens and how to prevent it. Third, implement a security plan and educate others in your organization. Take your responsibility by being a patriotic American and spread the word to other companies.

Information Technology (IT) personnel need to be involved in educating your company's employees on the methods of data breach and 'social engineering" used to fool them. Unfortunately, we are in a different world with different values. The fastest growing type of data theft is **insider theft and unauthorized computer access**. Your company may have spent millions in facility security and access but it is useless against inside theft.

Recognize the barriers to taking action. The idea that it "happens to other corporations" is based on the importance and profitability of your corporation in the marketplace, luck and time. You will have to spend some money. View your cyber and computer security technology as improvements in its proper framework; by comparing your investment to the cost of losing your intellectual property and operating data. Protect your future viability.

For more information you can visit www.thevaultpc.com on computer security. A downloadable Secure Data IP Plan for Government, Industry and Business is available on the 'Secure Data Storage' page here, and one for Healthcare and Insurance is on the 'US Government, CJIS and HIPAA' page here.

Losing Intellectual Property is bad but losing data that is subsequently used against you is far reaching and permanent. Once your company is hit - it is too late. Your company is part of America's economic security and sustainable future. Do something about it.

For questions or additional information visit the 'Contact Us' page on the link here.

Jim Austin
904.254.0849
www.thevaultpc.com