Special Report: Cyber Security — A Seriously Growing Problem

So much to cover. So little space and so little time.

Most experts will tell you it's not ***if*** your company — or you as a person — will be hacked and have your stored, private information and that of your clients, compromised.

It's ***when***.

A report a couple of weeks ago from Hold Security says a Russian gang has stolen 1.2 billion Internet logins and passwords and more than 500 million email addresses from 420,000 websites.

U.S. Assistant Attorney General for National Security John Carlin said the problem — obviously — is growing. "The threat is real, it is here, and it is not going away. The list of threats out there is significant and it is expanding."

He says in spite of all of the publicity for the attacks at Target, eBay and other major corporations, we are just not prepared as a companies and individuals for these attacks. This report — and conclusion from the 9/11 Commission's report on the 10th anniversary of its original terrorism report — agrees.

"We are at September 10th levels in terms of cyber preparedness. Companies' most-sensitive and patented technologies and intellectual property, U.S. universities' research and development, and the nation's defense capabilities and critical infrastructure, are all under cyber attack," the commission said.

Insurance has been thrust front-and-center into the cyber security debate and cyber insurance — other than maybe pet insurance — is the fastest growing insurance line in the world. And cyber insurance grows to more prominence and importance every day.

Target last week said it reached its coverage peak of $90 million for the attack it experienced during the holidays last year. The cost to the company is said to hit $235 million so it's losses will be tremendous.

As noted at the beginning of this report, it's not if you'll be hit but when.

ABI is a research company and one of many doing cyber danger studies. It recently released a report titled ***Cybersecurity Technologies Market Research***. The report

said these people are getting very, very good and as their skills improve, the danger increases.

The growing number of attacks means there is now a tremendous market for data loss prevention products. The industry will make $1.7 billion this year and it will likely increase by leaps and bounds next year and into the future.

ABI said in 2013 over 800 million records were compromised in theTarget eBay, Target, AT&T, Facebook, YouTube, Twitter and LinkedIn — and others — data breaches. And those are the ones we know about. A lot of breaches are never reported and the consumers involved are not notified and do not know their identities, passwords and personal information has been compromised.

The problem has reached the stage where many are insisting on government action. The U.S. House and Senate have passed cyber security bills that are similar and that are getting agreements by those who worry about privacy issues in government data breach sharing.

Whether the two bodies can get together and agree on one bill is anybody's guess.

At two cyber security meetings in Las Vegas a couple of weeks ago, cyber security was a hot topic. The bottom-line from speakers is that government needs to do more. There were suggestions of requirements for detailed reporting on cyber breaches like those required for deadly diseases by the Centers for Disease Control and Prevention (CDC) and the need for stress tests like Dodd-Frank is requiring for banks.

Another suggestion is for insurers to set "reasonable" prices for cyber insurance.

Insurance price — as you know — is set according to the risk. When it comes to cyber risks risk managers are on top of it. An organization called Data Breach Today said more than 750 million files were hacked last year. It's 50 million less than the ABI stats we quoted earlier.

So is it 750 million or 800 million? Or does it matter? It's a lot.

Crawford & Co. did a study of the six highest cyber risks:

Internal IT Enterprise: That is hardware, software, servers and people and process related to them. Dependence and interconnectedness of businesses and corporations, banks, joint ventures, industry associations and more is the issue.

Outsourcing and Contracts: IT and cloud providers, human resources, legal and accounting services, consultants, etc. mean risks for sharing cyber attacking bugs.

Supply Chains: This is self-explanatory. Firms that work together share the risk of infecting each others systems.

Disruptive Technology: New technology or existing technology that is not well understood. These are things like the Internet of Things, smart grids, embedded medical devices and so on. Employees not understanding them can lead to mistakes that lead to cyber attacks.

Upstream Infrastructure: Disruption to business and economies and society from hacking. Attacks on financial systems, telecommunications and electricity are a high risk for risk managers.

External shocks: These are risks outside of the system and that are out of the control of an organization. Things like an international conflict, malware etc.

One of the most seriously easy ways for malware to get into a business' server and computer system is USB devices like thumb drives, a computer mouse or keyboard. Security expert for SR Labs in Berlin Karsten Nohl said, "You cannot tell where the virus came from. It is almost like a magic trick."

Once a computer gets infected through that source — Nohl added — it then does others. "Now all of your USB devices are infected. It becomes self-propagating and extremely persistent. You can never remove it."

And that leads us to a warning from the U.S. Department of Homeland Security about a new malicious software. It attacks point-of-sales systems and is called ***Backoff***.

It steals information from payment cards like credit cards or debit cards and is very difficult — if not impossible — to detect by your anti-virus system.