# Special Report:
# Insurers & Cyber Risk

One of the industry's growing lines of insurance is cyber security insurance. The more cyber attacks we see, the more popular cyber insurance becomes.

There was a roundtable on cyber risk at the recently finished annual meeting of the Property Casualty Insurers Association of America (PCI). The conclusion of the panel is that insurers have a big role to play in helping other industries and companies combat the problem.

One of the speakers — Michael DuBose, the founder and president of the cyber defense firm CyDefense L.L.C. — said the insurance industry can do a lot to convince businesses that their data is not safe. "There is no such thing as 100%-secure network," he said.

And with that Dubose said there are just two types of companies, "those that have been hacked and those that will be." After making that statement, Dubose corrected himself and added it's really "those that have been hacked and know it and those that have been hacked and don't know it."

He suggests insurers advise companies to take three steps to amp up protection — and these are things insurers can and should do, too:

- Have a security firm do a thorough security audit.
- Set up an incident response plan that all levels of your organization agree to.
- Set up a system that delineates clearly who can access data and who cannot.

Dubose said, "Make sure that somebody in your organization knows where the most sensitive data is. During our investigations, we are often struck by how many organizations don't know who has the keys to the kingdom."

In the same session former Secretary of Homeland Security Michael Chertoff said cyber risk affects all of us — large business, small business groups and individuals. The threat comes from just about everywhere; from terrorists from inside this nation and out, to people who just enjoy the thrill of hacking, to disgruntled employees and customers, to accidents.

What all agree on is that any kind of data breach is devastating for the company involved and its customers or those in its database. In his speech, Chertoff said insurance can help alleviate the problem by sharing information, educating companies and the public and by establishing best practices and risk management solutions.

He said it is high time to develop cyber standards.

It's something the federal government is looking at doing. The Department of Commerce's National Institute of Standards and Technology (NIST) — a non-regulatory entity — has gotten input from 3,000 industry and education experts. It has drafted voluntary standards from that input.

The idea is protection without expensive regulations. President Obama ordered the NIST to do the work because Congress can't seem to agree on cyber security legislation.


Patrick Gallagher

The NIST document tells companies how to identify and protect the assets in their networks and how to detect a cyber attack, respond to it and recover from a breach. The details include keeping inventory of software platforms and applications, making sure top execs in a company know their responsibility and role when it comes to information security.

NIST Director Patrick Gallagher said the draft is a living document and one that will be flexible. "Ultimately what we want to do is we want to turn today's best practices into common and expected practices."