Update — The Raging Cyber Security Battle

As we all know, cyber security is becoming a huge problem in the U.S. The threat of attacks by hackers stretch from government to business to individuals and their personal computers.

And these criminals are growing more and more successful and more and more dangerous by the day.

Individuals and groups are screaming at government and industry to do something to stem the bleeding. Proposed solutions are loved by some and hated by others. That sets up a different sort of paralysis.

The U.S. Senate Intelligence Committee just passed a bill to help. Basically the bill calls for companies to exchange information with the government on threats to be hacked, attempts to get hacked or on actual hacking events.

Some worry about such sharing turning into an invasion of privacy by the U.S. government. And considering the spying done by the NSA and other government agencies the concern is valid. However, co-sponsors Sen. Diane Feinstein — a California Democrat — and Republican Sen. Saxby Chambliss of Georgia say this is the best chance we'll see of passing something that gets government and business cooperating on this issue.

"Cyber attacks present the greatest threat to our national and economic security today, and the magnitude of the threat is growing. This bill is an important step toward curbing these dangerous cyber attacks," Feinstein said.

Here's some good news. There is rare bipartisan support for the Senate bill in the House. Michigan Republican Rep. Mike Rogers and Maryland Democrat Rep. Dutch Ruppersberger are urging Senate members to pass the bill and they said they'd shepherd the bill through the House where they think it'll pass.

"We are confident that the House and the Senate will quickly come together to address this urgent threat and craft a final bill that secures our networks and protects privacy and civil liberties," the two said in a statement.

Here's some of what is in the bill:

- It authorizes companies and individuals to monitor their own systems and those of consenting customers for signs of hacking.

- It authorizes companies and individuals to share that information with the government.
- Data from cyber threats or cyber attacks will be stripped of personal identification information before it is shared with the government or with companies sharing with each other.
- The Department of Homeland Security must set up a system to increase the amount of cyber threat information it shares with business.
- Liability protections are in the bill to protect companies and individuals.

While the federal government looks at solutions the Securities Industry and Financial Market Association (Sifma) is wanting to create — what essentially is — a business-government war council on cyber security. The council will have eight government agencies including the Treasury, the National Security Agency and the Department of Homeland Security and representatives of business.

And Sifma is serious.

It has hired former NSA director Keith Alexander to head up the council creation and he's brought in top help like Michael Chertoff who is a former head of the Department of Homeland Security.

Sifma issued a statement on the proposal and said it is not optimistic that industry and government can withstand the non-stop, nearly withering attacks. The group said not only is business, industry and government vulnerable but the very infrastructure of this nation is in danger; an infrastructure that is critical to all.

"The systemic consequences could well be devastating for the economy as the resulting loss of confidence in the security of individual and corporate savings and assets could trigger widespread runs on financial institutions that likely would extend well beyond the directly impacted banks, securities firms and asset managers," Sifma said.