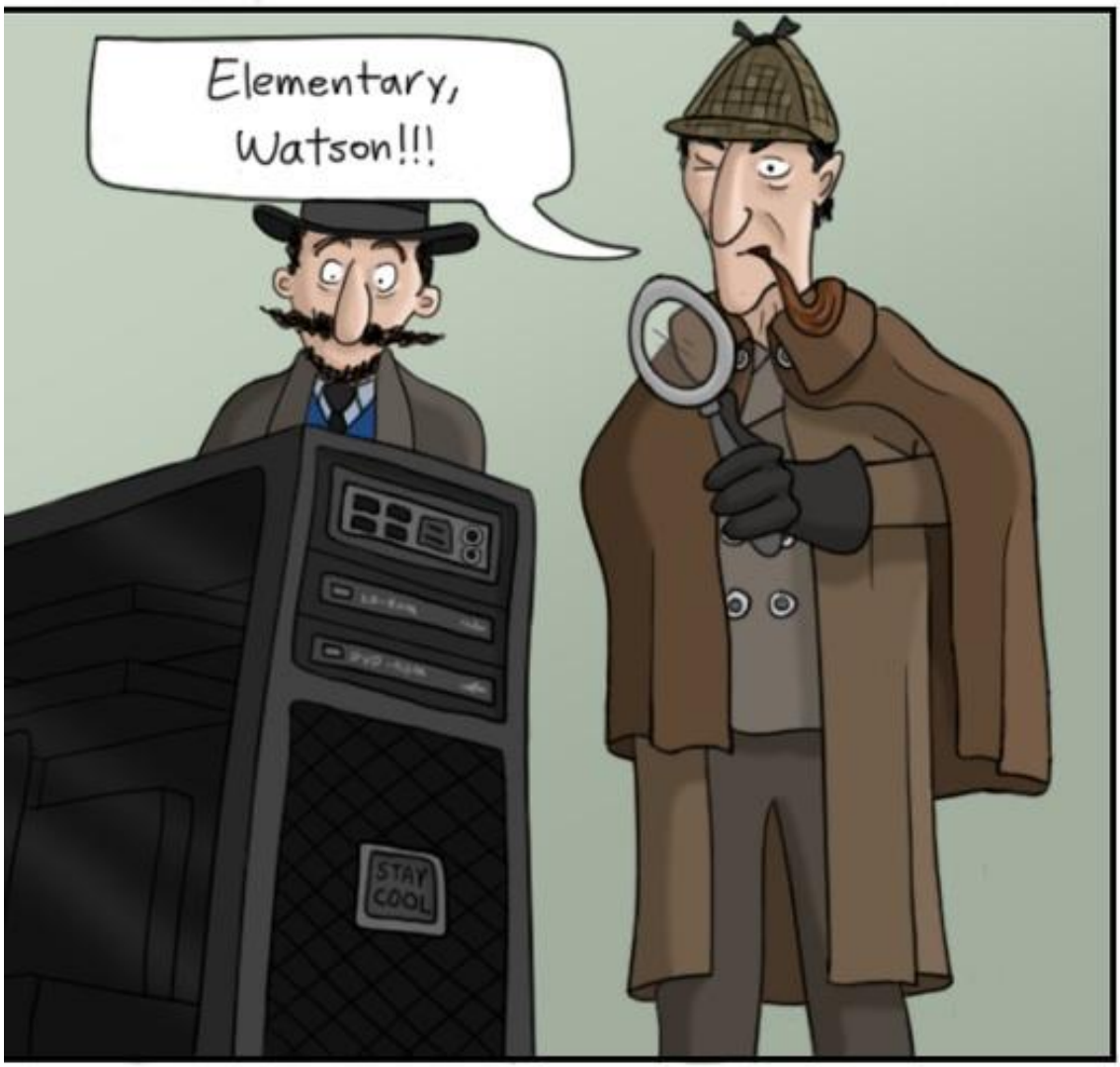
Judd Gregg, a former US Senator from New Hampshire and current head of he Securities Industry and Financial Markets Association, comments on cyber security in Bloomberg.

The financial industry has been under a constant state of attack for the past year as hackers attempt to steal clients' money, crash computer systems and disrupt capital markets. So far, the industry has been able to thwart the most serious attacks and protect its clients, but hackers are adapting and growing more dangerous.



Network forensics: the modern-day Sherlock Holmes.

It is vital that Congress recognize the urgency of this situation and take action to provide the private sector with the tools and support it needs to defend the millions of Americans it serves every day.

One of the most alarming trends is the increasing number of cyber-attacks on smaller financial institutions and businesses. These organizations typically don't have the same resources or access to information that larger companies do. This makes them more

vulnerable to a malicious attack that could disrupt capital markets and shake investor confidence in the financial system.

Hackers are also using individuals and smaller institutions as a gateway to infiltrate larger banking organizations. Everyone is a target.

Even in the absence of congressional action, cybersecurity is a top priority for the financial industry. It is devoting significant resources to build infrastructure and develop processes that protect clients, companies and the integrity of capital markets.

Evolving Threats

My trade group, the Securities Industry and Financial Markets Association, is organizing an industrywide exercise called "Quantum Dawn 2" on July 18. This exercise will simulate a cyber-attack on the U.S. financial system. It will force individual companies to test their response plans in order to maintain effective and orderly markets and protect client data.

The simulation will include more than 50 companies and exchanges, as well as the U.S. Treasury Department, the Securities and Exchange Commission and the Department of Homeland Security.

Industry efforts alone are insufficient. President Barack Obama got it right in his Feb. 12 executive order, which encourages partnerships between the federal government and private-sector businesses. But we need more information from the U.S. government on the diverse and evolving threats we are facing. Moreover, this information must be timely and actionable. The government has the resources to gather, process and disseminate intelligence on cyberthreats. Unfortunately, most of the time it can't share that information with the private sector until after a cyber-attack has occurred. The industry needs access to this threat information before an attack so it can proactively prepare and defend clients' information and assets.

Likewise, if a financial company is the target of an attack -- whether successful or not -- or has intelligence on a new threat, that information must be shared with government agencies and other companies that could be affected. Yet companies are cautious about sharing threat information that could be used to stop future attacks. Why? Currently there are no liability protections for companies that share pertinent data. That has to change. As Treasury Secretary Jacob Lew recently noted we need Congress to pass legislation that encourages and simplifies the flow of information between the government and the private sector.

Done right, information-sharing is the best way to keep our clients protected and our companies enabled to defeat the most critical threats. For example, last month, Microsoft Corp. and the Federal Bureau of Investigation successfully coordinated the global takedown of a ring that raided bank accounts around the world and netted more than half a billion dollars.

Critics of information-sharing say that the practice raises too many privacy concerns. These are unfounded: The industry takes client privacy very seriously and only shares information when absolutely necessary to address a threat. It also makes every effort to keep shared data anonymous.

Ensuring Privacy

The reality is that we are dealing with attackers who have no respect for privacy and will try to access and exploit client information by any means. To not share threat information would be like a citizen witnessing a robbery and not reporting it to the police: Nobody gains.

Common-sense legislation would promote information-sharing, update the criminal penalties associated with cyber-attacks, and provide protections for companies that share information and respond to malicious activity. Of course, legislation must also ensure the privacy of information that flows between companies and the government.

The government, the private sector and all Americans must remain vigilant in the face of cyber-attacks. The time is right for Congress to pass legislation that will ensure the resiliency of the economy as we navigate this new frontier of criminal activity.