War on the Internet

Cyber Security: Coming to a Computer Near You

By Jack Garson

August 2011 – As seen in the SmartCEO Magazine.

Cyber Security: Coming to a Computer Near You

In the past year, the computer virus called Stuxnet was launched upon the Iranian nuclear development program and is widely reported to have wreaked havoc, at least temporarily, on the Iranian centrifuges enriching uranium. This was a game-changer and wake-up call all in one. There have been militaristic skirmishes on the internet before. But this was an attack – not much different in impact than launching missiles at a country's weapons program.

More recently, hackers continue to attack the email accounts of government officials, steal data from multinational businesses such as Google, Sony, and Citibank, and probe the firewalls of defense contractors and vital infrastructure facilities in the United States. Both our president and Congress have woken to the threat not merely to government institutions, but businesses that keep our economy and country running.

A Wake-Up Call

For years, there have been both private industry standards and best practices for cyber security measures. The U.S. government has also issued cybersecurity guidance for its own operations that has been adopted by the business community. However, these requirements have been essentially voluntary for private companies. Then, in May 2011, President Obama's administration presented Congress with proposed new legislation that would begin to tackle the growing cyberthreats. In addition to requiring businesses to notify consumers if their personal data had been hacked, this law would impose new penalties for computer crimes, build public-private partnerships to protect sensitive electrical and other U.S. infrastructure and increase the Department of Homeland Security's role in tackling cyber security.

Congress is also responding to the threat. In June 2011, Congressmen Mc-Caul and Lipinski introduced the Cybersecurity Enhancement Act of 2011. Similar to the president's proposal, this law would impose rigorous standards on government systems and foster cooperation between the government and private enterprise in beefing up critical infrastructure, especially utilities, power grids, financial institutions and air traffic control systems. Other legislation currently being considered in

Congress includes the Grid Reliability and Infrastructure Defense Act. This law seeks to protect electric grids from a variety of threats, including cyber attacks.

Still, other government officials are formulating policies and strategies to address cyber attacks. Recent reports indicate that the Department of Defense will clarify its position that cyber attacks on certain facilities will be considered acts of war that could be met with physical retaliation. As one widely quoted defense official declared, “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.”

How It Affects Your Business

While the initial response is light on the regulation of businesses, that may change – dramatically. Battle lines are being drawn. Our government could merely encourage battle-hardening of computer systems by private enterprises. Or new laws might mandate that businesses implement cyber security measures and penalize companies for failing to do so. We are in the early stages of policy-making, and proposals are springing up on both sides of this divide.

The Light Touch: Many officials are pursuing the regulation-lite approach. They would not require operators of critical infrastructure, or any other businesses, to adopt specific cyber security measures. Rather, these regulators want to encourage businesses to implement cyber security technology and then aid them in doing so. President Obama’s proposed law largely takes this approach. The president’s initiative would also audit critical infrastructure operators against an industry-specific set of standards and publish the audit results. This approach seeks to drive customers to do business with companies that bolster their cyber defenses. It is hoped that if companies neglect cyber security, their customers would take their business elsewhere. However, such market forces may be of limited benefits if a business, such as a utility, operates with monopoly type bargaining power, as is the case with certain infrastructure owners.

Still others in government want to go further and free businesses from existing local requirements, as well as liabilities that already exist. For example, dozens of states have already enacted a variety of laws that impose various cyber security requirements on businesses. Recent federal legislative proposals include elimination of the state-by-state quilt of cyber regulation that is now sprouting up. Further, Senators Collins and Lieberman recently suggested that the president’s proposed legislation should also include liability protection for those businesses that implement security measures but still fall prey to cyber attacks.

However, others cite the recent debacle on Wall Street and the constant pressure companies face to maximize their bottom line as reasons for mandatory cybersecurity measures.

The Heavy Hand: Many officials advocate a rigorous regulatory approach, arguing that if cybersecurity is not required, it won’t be widely implemented. These advocates call for specific cyber security obligations and penalties for noncompliance. For example, one prominent former defense official suggests that the Department of Homeland Security should be able to require the private owner of a critical infrastructure to implement specific cyber security measures within a given time frame or face

stiff penalties. Similarly, proposed legislation would require companies in particular industries to create network protection plans that would be subject to regulation by the Department of Homeland Security.

However, the possibilities and strategies for mandatory cybersecurity, as well as the unintended consequences, are virtually limitless. Just last year, certain senators floated a legislative trial balloon that would create an “internet kill switch,” authorizing the president to shut down the internet throughout the United States in a national emergency. After an outcry over the widespread potential consequences, this idea was abandoned. But the search for effective cyber security proceeds.

Further, the idea of mandating specific cyber security measures has been criticized because threats evolve and required cyber security measures may become swiftly outdated. The research and development arm of the cyber attackers is robust, with new methods of intrusion being developed on a regular basis.

Staying on The Cutting Edge

Sitting and waiting for someone to hand you new legal requirements over the next few years may produce your own series of expensive and disruptive wake-up calls. You can take action now:

- Monitor the legislative debate as ideas become requirements so that you will be prepared to comply.

- If you run a company especially close to cyber threats, such as a utility provider or transmitter, a defense contractor or a security firm, get involved in the discussion with your legislators.

- Make cyber security measures part of your competitive edge. There is already extensive guidance from the ISO (International Organization of Standardization) to NIST (the National Institute of Standards and Technology) to various private industry associations that produce cybersecurity guidance. Early adopters offer their customers an advantage that may translate into more business and, likely, more secure operations.

Plenty of businesses have long recognized the risk presented by loss of power or equipment failure. So they have implemented precautionary measures like backup generators and redundant off-site storage of computer data. Cyber war now presents the same threat that calls for new security measures. Be prepared.

Jack Garson is the founder and a principal of the law firm Garson Law LLC in Bethesda, MD, and is also the author of “How to Build a Business and Sell It for Millions.”

Jack Garson
Garson Law LLC
(301) 280-2700
jgarson@garsonlaw.com