msk

new cybersecurity law – are you prepared?

MSK Client Alert

January 11, 2016

On December 18, 2015, President Obama signed into law the Cybersecurity Act of 2015. Beginning at Division N, Public Law 114-113 deals with cyber threats and includes the framework for the means and methods by which the private sector may submit such information to the government and by which the government is intending to share comparable information with the private sector (and others). The actual processes will be put together by the Director of National Intelligence along with the Secretaries of Commerce, Defense, Energy, Homeland Security and Treasury, plus the Attorney General, a process which is to be completed and submitted to Congress no later than February 16, 2016, so we will know soon enough what will occur.

The antitrust protection of the new law is limited to disclosure of cyber threat indicators or information that is exchanged or assistance that is provided with "facilitating the prevention, investigation, or mitigation of a cybersecurity threat" for information stored, processed or passing through a system.

Information sharing is to extend beyond the private sector to also include non-federal government agencies or departments and state, tribal and local governments. The information sharing itself is supposed to extend to cybersecurity threats to prevent or mitigate adverse effects. The form of sharing is to be periodic, through publication and targeted outreach, of cybersecurity best practices developed based on on-going analyses of cyber threat indicators, defensive measures and so on. According to the new law, attention will be given to the accessibility and implementation challenges faced by small business concerns. In theory, the information sharing is to be in real time (but do not assume it will be instantaneous), but there are provisions which allow for delay in the sharing of the information, for example for national security reasons or to remove information that identifies an individual.

What this new law reminds all companies is to be prepared. There are key pre-breach and post-breach factors to consider in putting together your plan. We

attorneys

Susan Kohn Ross

practice areas

cybersecurity and privacy

regulatory

recommend the following:

Pre-Breach Issues/Measures

- Regulatory Framework/Standards.
- Vulnerability Assessments/IT Protections.
- Training and SOPs (frequent training, regular SOP reviews and updates, backup and testing, strong passwords, physical access controls, limits on the use of USB drives).
- Emergency Preparedness Plan to include outside supporting experts, including counsel, technology and insurance.

Post-Breach Crisis Management

- Secure Your System
- Contact Counsel, Insurer, PR Team, and possibly Law Enforcement
- Comply with Data Breach Notification Laws
- Implement Your Preparedness Plan
- Preserve evidence/do not turn off computers.
- Confirm what data you have and what is on or off-site in the hands of third parties, including employees and vendors.
- Complete a forensics investigation to determine the nature and severity of the incident; who leads? who staffs?
- Implement your emergency preparedness/business continuity plan – who says what to whom, when and how?
- PR: Tell the truth without creating judicial admissions; maintain control over the information and your credibility.
- Bring in an expert to interact with the government and the media (Counsel, PR and IT).
- Reevaluate/reassess your emergency response plan and insurance coverage.

Whether or not you sell products/services on your website, you need to be prepared. It makes no difference what industry you are in, whether you are regulated by any federal or state agencies, or whether your industry has been subjected to a guidance document from any regulatory agency or commercial organization, the reality is that every company is at threat to be hacked. If you have not already prepared your plan, now is the time to do so.

If you have a plan, when was it last updated? When was the last time your team trained on it?

There are two primary sources of potential headaches – having your data in the cloud and having your provider hacked, or you yourself being hacked. Either way, it is a recipe for disaster if you have not figured out how you will respond before the crisis arises. Keep in mind, if the device can be connected to the Internet, it is susceptible to be hacked!

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899