Tatiana Melnik

New U.S. Sanctions Program Seeks to Give Government an Extra Tool to Fight Cyber-Attacks

Health Care Organizations Must Familiarize Themselves with OFAC Requirements and Implement Appropriate Internal Controls

Tatiana Melnik is an attorney focusing her practice on information technology, health care, data privacy and security, regulatory compliance, and general business matters. Ms. Melnik regularly writes and speaks on HIT legal issues, including cloud computing, HIPAA/HITECH, BYOD, and data breach reporting requirements. She is a managing editor of the Nanotechnology Law and Business Journal and a former member of the Michigan Bar Information Technology Law Council. Ms. Melnik is admitted to practice in Florida and Michigan. Ms. Melnik holds a JD from the University of Michigan Law School, a BS in Information Systems, and a BBA in International Business, both from the University of North Florida. She can be reached by phone at 734/358-4201 or by email at tatiana@melniklegal.com.

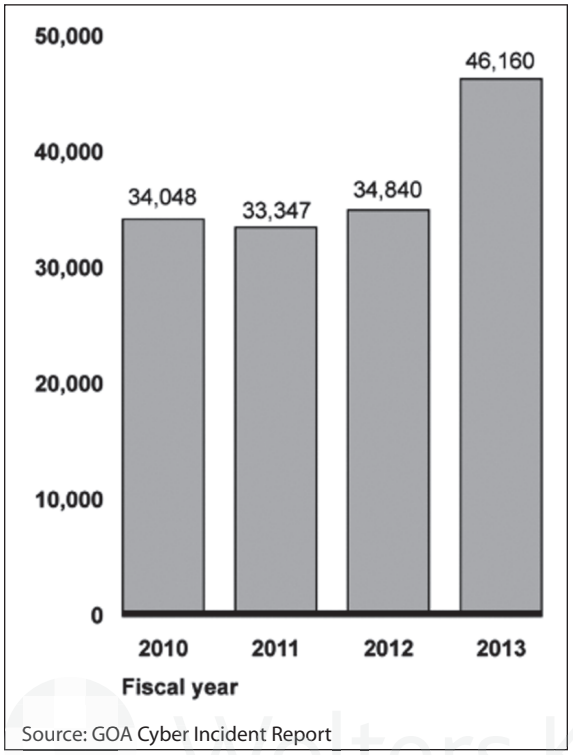
On the heels of cyber-related data breaches at Anthem, Inc., Premera Blue Cross, and Sony Pictures, President Barack Obama signed an Executive Order on April 1, 2015, seeking to give government officials a new tool to address "malicious cyber-enabled activities" by imposing sanctions on foreign persons and entities responsible, as well as those individuals — both foreign and domestic — providing assistance to such foreign persons or entities.[1] Executive Order 13694[2] establishes a new sanctions program, which is designed to financially target and deter parties engaging in, profiting from, or in any way supporting the actors engaging in these malicious cyber activities, which the Executive Order identifies as an "unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[3]

Increase in Malicious Cyber-Related Activities

The general consensus is that cyber attacks against both U.S. government agencies and private companies continue to increase in number.[4] For example, between 2010 and 2013, the number of cyber incidents against U.S. federal agencies increased by about 35 percent, from 34,048 in 2010 to 46,160 in 2013.[5] The 2013 numbers were about 32 percent higher than the number of cyber incidents in 2012 (34,840).[6] (See Figure 1)

The private sector has seen similar increases in cyber incidents; however, the numbers are significantly higher as compared to the U.S. government numbers. According to PricewaterhouseCoopers' (PwC's) annual *The Global State of Information Security® Survey 2015* (the "report"), "the total number of security incidents detected by [the

Figure 1: Cyber Incidents Reported to US-CERT by All Federal Agencies: Fiscal Years 2010-2013.



Source: GOA Cyber Incident Report

9,700+] respondents climbed to 42.8 million [in 2014], an increase of 48% over 2013," for which respondents reported 28.9 million incidents.[7] The motivation for these attacks ranges from cyber crime, to cyber espionage, to hacktivism, to cyber warfare. Whatever the motivation for an incident, the financial loss associated with a data breach is also generally increasing, with the largest increases being felt by the largest organizations. According to the PwC Report:[8]

- Large organizations — those with revenues of over $1 billion — reported that the financial losses attributable to the cybersecurity incident increased from $3.9 million in 2013 to $5.9 million in 2014.
- Mid-size organizations — with revenues between $100 million and $1 billion — financial losses attributable to the cybersecurity incident remained relatively steady but increased from $1.0 million in 2013 to $1.3 million in 2014.
- Smaller organizations — those with revenues of under $100 million — reported that financial losses attributable to the cybersecurity incident *decreased* from $0.65 million in 2013 to $0.41 million in 2014.

Many of the cyber attacks are being launched by persons and entities located outside of the United States. For a real-time view of both attack origin as well as attack target countries, see the Norse Live Attack Map at map.ipviking.com, which is compiled based on Norse's 8 million global sensors. The Executive Order is designed to provide the U.S. government with additional resources to fight malicious cyber incidents undertaken by parties outside of the United States.

About the Executive Order and the SDNs List

Executive Order 13694 establishes a new sanctions program and grants authority to the "Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State," to impose sanctions on individuals and entities that are found "to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are *reasonably likely to result in*, or *have materially contributed to*, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States that have the purpose or effect of:"[9]

1. harming or otherwise significantly compromising the provision of services by a computer or network of computers that support one or more entities in a critical infrastructure sector;
2. significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
3. causing a significant disruption to the availability of a computer or network of computers; or
4. causing a significant misappropriation of funds or economic resources, trade

> secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain.[10]

Specifically, the Executive Order grants the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, the authority to add individuals and entities engaging in malicious cyber-enabled activities to the Specially Designated Nationals and Blocked Persons (SDNs) list, which is managed by the Treasury's Office of Foreign Assets Control (OFAC). OFAC administers and enforces U.S. economic and trade sanctions against targeted foreign countries, regimes, terrorists, narcotics traffickers, and other actors deemed as threats to national security, foreign policy, or the U.S. economy.

In general, the assets of individuals identified on the SDNs list are frozen, and U.S. persons and entities are, with some exceptions, prohibited from doing business with them. Organizations must take care to comply with the requirements because the penalties can be quire severe. As OFAC explained:

> The fines for violations can be substantial. Depending on the program, criminal penalties for willful violations can include fines ranging up to $20 million and imprisonment of up to 30 years. Civil penalties for violations of the Trading With the Enemy Act can range up to $65,000 for each violation. Civil penalties for violations of the International Emergency Economic Powers Act can range up to $250,000 or twice the amount of the underlying transaction for each violation. Civil penalties for violations of the Foreign Narcotics Kingpin Designation Act can range up to $1,075,000 for each violation.[11]

In March 2015, the Treasury announced a $7,658,300 settlement with PayPal, Inc. for violating trade sanctions against Iran, Sudan, and Cuba.[12] OFAC identified 486 transactions totaling $43,934 and initially calculated the penalty at $17,018,443, which amounts to a penalty of $35,017.37 per transaction.[13] But OFAC reduced the fine because PayPal self-reported the violation, hired new management for its compliance group, and cooperated with the investigation. The final settlement amounts to a penalty of $15,757.82 per transaction.[14]

Take-a-Way for Health Care Organizations

The health care industry has been identified as a "critical infrastructure sector," and therefore, malicious cyber attacks against payors, hospitals, and other organizations in the health care space would qualify for action under the Executive Order. As the health care industry increasingly becomes the target of malicious cyber-related activities, health care industry leaders must take a more active approach to protecting their information technology infrastructure. At the same time, as many health care organizations seek to expand their global footprint, they must familiarize themselves with OFAC requirements and ensure they have implemented appropriate internal controls to comply with prohibitions on doing business with individuals and entities that may be identified as SDNs or are otherwise sanctioned under U.S. laws.

Endnotes:

1. Exec. Order 13694, 80 Fed. Reg. 18,077 (April 1, 2015), available at www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf [hereinafter Executive Order].
2. *Id.*
3. *Id.*
4. *But see* Paolo Passeri, *2014 Cyber Attacks Statistics (Aggregated)*, Hackmageddon.com, Jan. 13, 2015, hackmageddon.com/2015/01/13/2014-cyber-attacks-statistics-aggregated/ (last visited April 5, 2015) (data demonstrating that the number of cyber incidents for 2014 were less than the number of incidents for each of 2012 and 2013, with cyber-crime being the primary motivational factor).
5. Government Accountability Office, Information Security: Agencies Need to Improve Cyber Incident Response Practices, Figure 1: Cyber Incidents Reported to US-CERT by All

Federal Agencies: Fiscal Years 2010-2013 (April 20104) ("During fiscal year 2013, agencies reported a total of 61,214 incidents to US-CERT, which were comprised of 46,160 cyber incidents and 15,054 non-cyber incidents. According to US-CERT, a 'non-cyber' incident is one that involves the mishandling of sensitive information without a cybersecurity component, such as the loss of a hard copy record containing personally identifiable information. Cyber incidents are the focus of this report."), available at www.gao.gov/assets/670/662901.pdf [hereinafter GOA Cyber Incident Report].

6. *Id*.
7. PriceWaterhouseCoopers, Managing Cyber Risks in an Interconnected World: Key findings from The Global State of Information Security® Survey 2015 p. 7 (Sept. 2014) ("The 2015 survey was conducted online from March 27, 2014 to May 25, 2014; readers of CIO, CSO, and clients of PwC from around the globe were invited via e-mail to take the survey … . The margin of error is less than 1%.") available at www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml
8. *Id*. at 10.
9. Executive Order, *supra* note 1, §(1)(a)(i) (emphasis added).
10. *Id*.
11. U.S. Dept. Treasury, Resource Center: Frequently Asked Questions: How much are the fines for violating these regulations?, www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx#12 (last visited April 5, 2015).
12. U.S. Dept. Treasury, Enforcement Information for March 25, 2015: PayPal, Inc. Settles Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs (Mar. 2015), available at www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal.pdf.
13. *Id*.
14. *Id*.

Reprinted from Journal of Health Care Compliance, Volume 17, Number 3, May-June 2015,
pages 53–56, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.