athenainsight

Today's data. Tomorrow's healthcare. athenainsight.com

So you've been hacked? Now Uncle Sam will punish you, too.

By Stephanie Zaremba | July 29, 2016

Imagine a growing epidemic of burglaries affecting retail stores across the country. Business owners diligently stay abreast of the latest security technologies, upgrading their locks and expending ever-increasing resources to monitor for threats, but to no avail. As soon as the newest technology is implemented, the perpetrators find a new security weakness to exploit. In this never-ending race to the bottom, a break-in might be only a matter of time.

Now imagine that when businesses become victims of these crimes, they face six- or seven-digit penalties, a spot on a government "wall of shame," and a loss of credibility with customers.

That sounds absurd, right?

Unfortunately, this is exactly how the regulatory landscape is set up in healthcare today. As health information increasingly moved to electronic formats in the 1990s, Congress enacted the 1996 Health Insurance Portability and Accountability Act, or HIPAA. At the time, the legislation addressed a quickly emerging need: The healthcare industry had begun to store and exchange insurance claims and other health information electronically, so safeguards were needed to ensure that information was used and disclosed appropriately.

For much of the past 20 years, HIPAA — though imperfect — served its purpose well. The majority of HIPAA breaches were the result of what most of us would call stupid mistakes or a failure to follow known best practices — things like the lost laptop that stored unencrypted patient information or the employee who failed to dispose of patient records appropriately.

These HIPAA violations trigger a number of obligations on the offending party. They can result in fines totaling hundreds of thousands, if not millions, of dollars. And where HIPAA breaches are caused by negligence, these penalties can function as an important tool, incentivizing stewards of patient data to invest in appropriate privacy and security safeguards.

But in the past five years, criminal cyberattacks on healthcare entities have increased 125 percent. Cybercrimes are now the leading cause of health information breaches, replacing employee negligence and lost or stolen devices as the number one source.

A recent study found that 88 percent off ransomware attacks detected in the second quarter of 2016 affected healthcare. And Cisco's 2016 midyear cybersecurity report concluded that ransomware is now the most profitable type of malware in history — perhaps in part because health systems are more willing than other businesses to pay ransom to retrieve vital patient data quickly.

In response to this growing trend, the Department of Health and Human Services recentlyannounced a funding opportunity for an Information Sharing and Analysis Organization. The objective is to provide a forum for better dissemination of threat and response information to prevent future attacks.

This could be an important resource, but it raises a host of issues. And it ultimately highlights the need for Congress to revisit HIPAA altogether, in light of all that has changed in our information economy since 1996.

Congress needs to ensure that HIPAA requirements take into account our new reality: When a Medicare number can sell for as much as $500 on the black market, criminals have a strong incentive to outsmart even the most sophisticated security systems.

But right now, even when a healthcare entity could not have known it was violating HIPAA — as may be the case when the victim of a cyberattack — it still may be subject to government fines. And it still will face significant expense in notifying patients of the attack, paying for financial monitoring services, and dealing with fallout.

In situations where victims followed best practices, and could not have done more to prevent a cyberattack, the penalty structure needs to change. In addition, Congress needs to devise a system of safe harbors for cybercrime victims. Because as it stands, the potential for penalties is a strong disincentive for companies to share information about the threats they face. What if, as a victim, you share your experience, hoping others can learn from your mistakes, only to have Department of Health and Human Services turn around and slap you with penalties for those mistakes?

Healthcare systems need to stay up to date on cybersecurity protections. But they also need incentives to exchange information about weaknesses and best defenses — with other healthcare companies, and with the government. That's the ultimate way to keep hackers at bay, and to keep health information safe.

Stephanie Zaremba is director of government and regulatory affairs for athenahealth.