TECH MAY 17 2016, 1:48 PM ET

# Cyber Attacks and Negligence Lead to Rise in Medical Data Breaches

by HERB WEISBAUM

America's healthcare organizations are being attacked by data thieves, but the industry is not doing nearly enough to deal with the growing threat, according to a new study by the Ponemon Institute.

These breaches are "increasingly costly and frequent, and continue to put patient data at risk," the report concluded.

Key findings:

- Nearly 90 percent of the healthcare organizations surveyed had a data breach in the past two years
- Nearly half (45 percent) had more than five breaches in that time period
- The annual cost of dealing with these breaches is estimated to be $6.2 billion

"The industry has not made very much progress since we starting looking at this issue six years ago," said Dr. Larry Ponemon, founder of the Ponemon Institute. "Many organizations don't have the resources or the staffing to get the job done right. My prediction is that things are going to get worse before they get better, but they will get better."

Criminal attacks are the main cause of these the breaches, accounting for half of the problem, up five percent from last year. And many of these thefts are inside jobs. In fact, 13 percent of them are pulled off by someone inside the healthcare organization.

**Read More: Electronic Medical Records Are Latest Target for Identity Thieves**

The other half of the breaches can be attributed to sloppiness and employee mistakes — for example, losing a computer with unencrypted patient information on it.

“The problem is often not high-tech, but very low-tech,” Ponemon told NBC News. “It’s getting people who work in the organization to become smarter about data protection and privacy issues. There’s still a lot of carelessness and negligence. It’s good people doing stupid things.”

The American Hospital Association (AHA) told NBC News that the industry is taking action to deal with the growing threat.

“Cyber criminals are targeting information systems in every sector. Hospitals are working very hard and are particularly vigilant about protecting their patients and data," Rick Pollack, AHA’s president and CEO, said in a statement. "Hospital leaders are using the lessons learned in previous attacks and are applying best cyber security practices shared by the AHA in an effort to anticipate and respond to existing and emerging threats.”

Rick Kam, president and cofounder of ID Experts, (which sponsored the Ponemon report) told NBC News he believes a lack of accountability in the healthcare industry is one reason the problem is getting worse.

“There’s a lot of finger-pointing going on,” he said. “They need to realize that part of patient care includes protecting patient data, because if health information is disclosed you can never put it back in the bottle.”

Things won’t get better until health care providers get back to the basics, Kam said. There needs to be better employee training, stronger mobile device policies, regular data risk assessment and enforceable internal procedures.

## Attacks go unnoticed, unreported

Nearly half the healthcare organizations and more than half of their third-party business associates in this study said they have “little or no confidence” that they can detect all of the lost or stolen patient data.

“That’s pretty scary,” Ponemon said. “They admit that a lot of data breaches are going to go unnoticed because they don’t have the right tools in place to identify and contain these breaches.”

**Read More: Hacking of Health Care Records Skyrockets**

The majority of medical breaches are small — involving fewer than 500 records — the report noted, so they do not need to be reported to the federal government and the media may never find out about them.

The healthcare providers and their business associates said they realize stolen medical records lead to various forms of identity theft. And yet, most don’t offer any type of protection services to patients who were victimized.

Pam Dixon, executive director of the World Privacy Forum, told NBC News there is no national law that tells a doctor, hospital or healthcare provider how to respond to a breach of patient information

“This has created chaos,” Dixon said. “Even when someone realizes this happened to them, it can be really difficult to clean up the mess. Sometimes the healthcare provider is really great about working with the patient, but other times the victim can’t even get a copy of their healthcare file.”

## Human cost of medical breaches

Medical identity theft is extraordinarily harmful to people, much worse than the breach of credit or bank account numbers. When those are stolen, you can close the account and move on with your life.

The damage that can result from stolen medical records can be significantly worse and harder to spot, and can last a lifetime. That's because your medical file is a treasure trove of sensitive personal information that an identity thief can use in various ways.

"Your medical records are the keys to the kingdom," said Eva Velasquez, president and CEO of the non-profit Identity Theft Resource Center. "The information in that file includes [your] Social Security number, often payment information, where you're going for medical care and where you're getting your prescriptions."

An identity thief can use this information to get medical treatment, medical equipment or prescription drugs in your name. That can result in bogus information being added to your medical file — and you may never spot it. All of a sudden your blood type changes or it looks like you had a surgery that you didn't have. The consequences of that, experts say, can be life-threatening.

In fact, the Ponemon study found that fifty-eight percent of healthcare organization and 67 percent of their business associates don't have a process in place to correct these errors in a victim's medical records.

And because medical records contain so much personally identifying information, they can be used to commit other types of fraud.

**Read More: Healthcare Way Behind on Data Security, Cyber Firm Says**

"The thief can do all sorts of things to monetize that stolen information," Velasquez told NBC News. "We believe these medical breaches have led to the explosion of IRS and state identity tax fraud."

We expect our medical providers to provide quality care. And we trust them to be good stewards of all the personal information, both medical and financial, that they have about us. But reports like the new one from Ponemon suggest that sometimes that trust is misplaced.

“The medical industry doesn’t understand the incredible value of the data they’re holding. When something is super valuable, you guard it, you protect it. They just don’t regard patient data as the extremely valuable commodity that it is,” Velasquez said.

If you think you might be a victim, the Identity Theft Resource Center has information on how to spot medical identity theft.

***Herb Weisbaum is The ConsumerMan. Follow him on Facebook and Twitter or visit The ConsumerMan website.***

---