



DEEP DIVE

Charts: Must-know healthcare cybersecurity statistics

The healthcare industry was the victim of 88% of all ransomware attacks in U.S. industries last year.

Published Feb. 27, 2017

By Ana Mulero

Associate Editor

*Want to read more on **cybersecurity**? Check out our comprehensive guide analyzing the cybersecurity trends and themes impacting healthcare in 2017 and beyond.*

No one is immune to to cyber attacks. Healthcare organizations are now dealing less with employee negligence causing health data breaches, but they are facing a substantially larger number of malicious threats to security.

The healthcare industry was the victim of 88% of all ransomware attacks in U.S. industries last year, according to Solutionary, an NTT Group security company. And 89% of studied healthcare

organizations have experienced data breaches which involved patient data being stolen or lost. Over the past two years, a report from the Ponemon Institute shows.

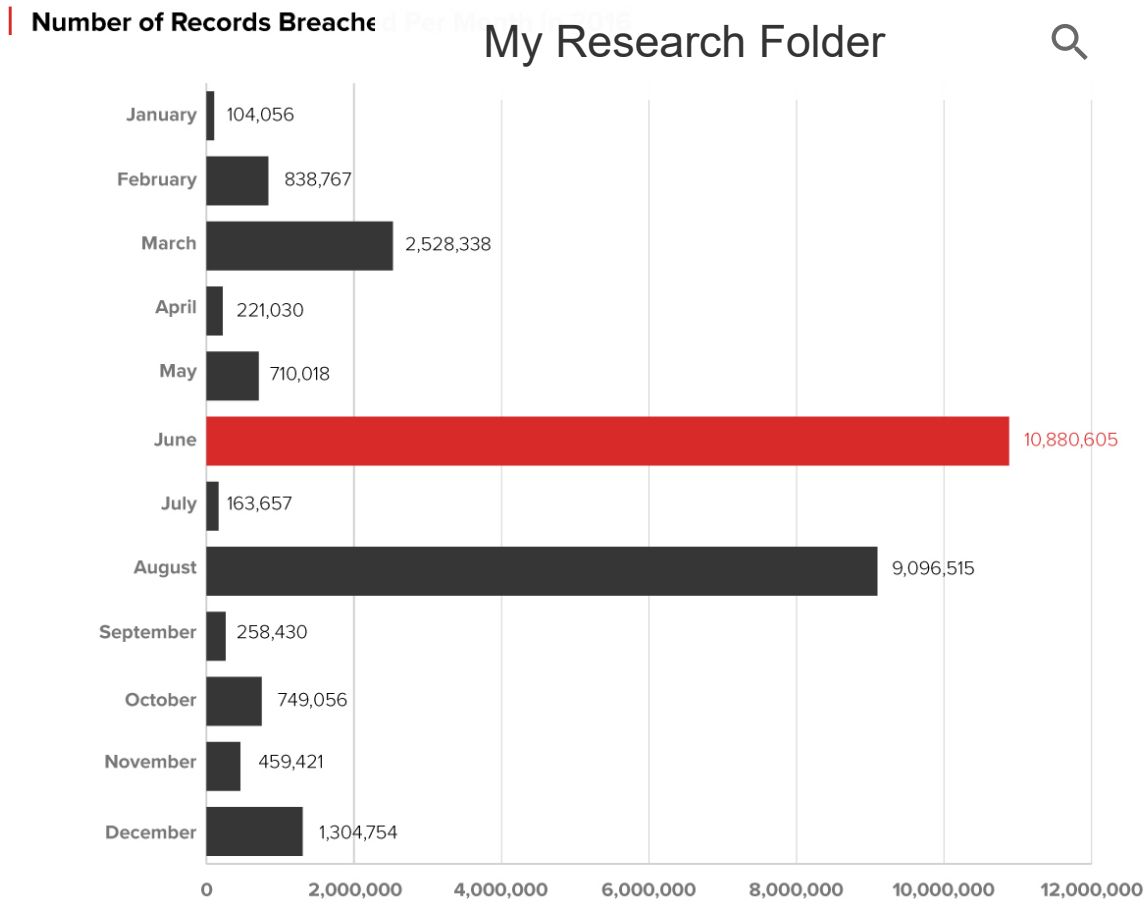
My Research Folder



Cyber criminals know healthcare organizations tend to pay the ransom amount that is demanded in return for patient data. A 2016 IBM survey found that 70% of businesses who have had experience with ransomware attacks in their workplace have paid to have stolen data returned.

While the type of security incident that many healthcare organizations continue to be concerned about is employee negligence, the technologies used in care settings also continue to have a multitude of cybersecurity vulnerabilities. Yet the industry is inadequately prepared to prevent and respond to these types of attacks. Tenable Network Security's 2017 cybersecurity report gave it a grade of 54% on risk assessment – down 18% from 2016. And Security Scorecard ranks the healthcare industry at 9th for its overall security compared to other industries.

The graphic below on health data breaches that have affected 500 individuals or more reported to the U.S. Department of Health and Human Services' Office of Civil Rights supports global information services group Experian's prediction that even more healthcare cyber and ransomware attacks will occur during 2017.



Source: Protenus, Inc. & DataBreaches.net


Healthcare Dive

In fact, this year has been averaging a health data breach per day, according to a new Protenus report.

However, healthcare cybersecurity data provide the insights needed to understand the scope of the problem and make the right decisions for protecting patients' electronic health information.

\$6.2 billion

Health data breaches are costing the U.S. healthcare industry an estimated \$6.2 billion, according to the Ponemon Institute.

My Research Folder 

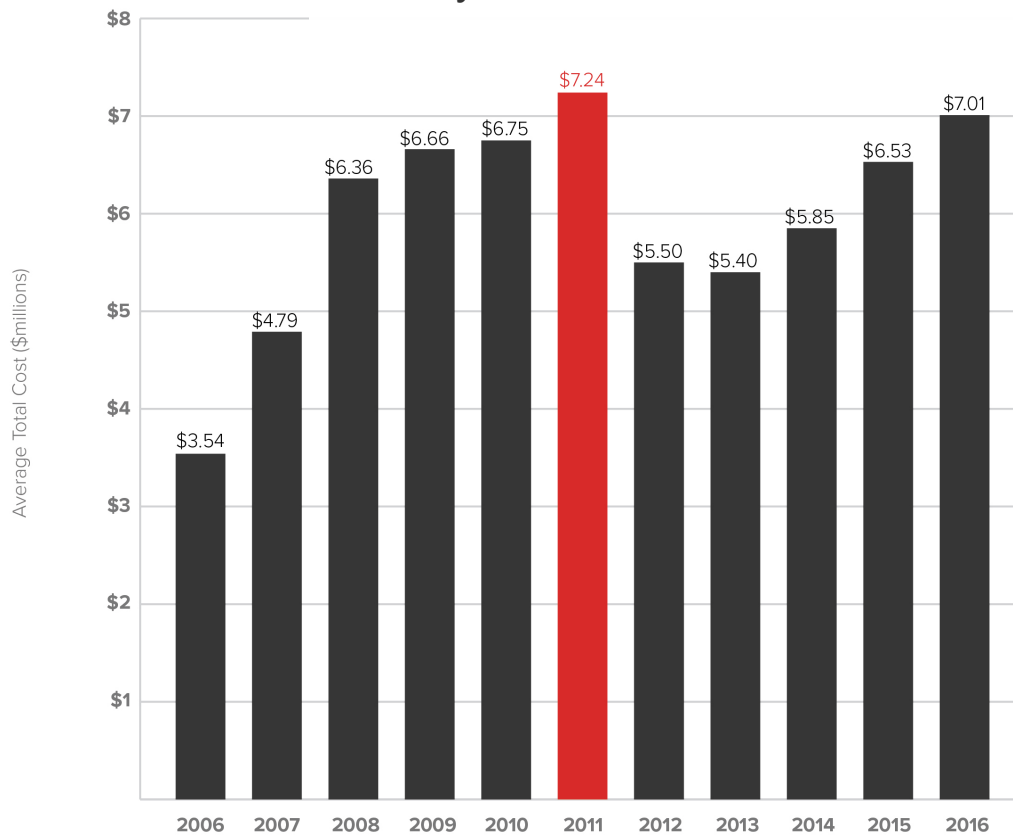
These breaches are costly for healthcare as it is among the heavily regulated industries that usually have a higher per capita cost of a data breach than the overall mean (\$221), a 2016 Ponemon report shows. A stolen electronic health record (EHR) cost the average business \$355 in 2016, a global analysis of data breaches adds.

“It is safe to say that costs to healthcare organizations will continue to rise as one of the fastest-growing threats, ransomware, successfully wreaks havoc in the industry,” the latest IBM X-Force Research report states.

The chart below illustrates how the average organizational cost of a data breach worldwide has increased:

The average total organizati

My Research Folder



Source: Ponemon Institute Research Report

Healthcare Dive

Months or more

While 56% of incidents in 2015 were discovered within several days, months or more went by before 39% of the studied healthcare organizations became aware of the breach, Verizon reports.

Healthcare systems are too often taking too long to discover security incidents and notifying victims. This is despite the fact that it took cyber criminals a few minutes or less to compromise

healthcare systems in
 successful attackers f
 potentially lucrative—patient records,” the report states.

Out of 16 different factors that impact the cost of a data breach in the U.S., the lack of a incident response team increases the cost the most - about \$25, IBM found. Patients are perhaps the most affected by these attacks as their personal health information can be exploited, disclosed, or otherwise misused. Yet companies still spend less on minimizing the risk of a breach and helping impacted individuals than they spend on efforts to notify victims and investigating the incident, according to IBM.

300%

Using OCR’s data, California-based TrapX Security found the total number of reported data breaches that impacted at least 500 Americans caused by cyber attackers spiked by about 300% from 2014 to 2016. There were more than 200 of these breaches last year, according to the OCR.

The month of June saw the largest number of stolen or lost records from a breach, a 2016 Protenus Breach Barometer report shows:



Healthcare Dive

Less than 6%

My Research Folder



While 16% of the 2016 federal IT budget was allocated for cybersecurity, the “healthcare industry averages are much lower, with less than 6%,” according to software company Symantec.

“Weak cybersecurity makes electronic protected health information (ePHI) more vulnerable,” the Symantec report states. The amount spent on healthcare cybersecurity today falls short of what is needed to protect ePHI. “Medical records contain most of the data hackers want, making them ideal for one-stop stealing,” the report adds. The company reported each chart on an EHR can sell for \$50 on the black market vs. \$1 for a stolen social security or a credit card number.

However, healthcare organizations are becoming increasingly aware of the bullseye on their backs and about 80% of them plan to increase their data security spending this year, a 2017 Thales Data Threat report shows.

3.6 million

Arizona-based Banner Health experienced the cyber attack that impacted the largest number of patients (3,620,000) last year, according to Trapx Labs. But the second largest healthcare data breach report, which occurred at Newkirk Products, headquartered in Albany, NY, wasn't too far behind, with a total of 3,446,120 individuals affected. A former Banner Thunderbird Medical Center

employee filed a class
the massive breach.

My Research Folder



The data from IBM X-Force research team show how the number of EHR breaches significantly varied by state in 2015:



Healthcare Dive