Three Data Breaches and What Might Have Helped to Avoid Them

Three Data Breaches to Consider

Data breaches are crippling to any business, but are extra hard on healthcare organizations, considering the vast amount of sensitive information consumers trust them with and the irreparable damage to reputation that can follow a breach. Healthcare entities are held to the highest trust standards, and face increasing federal and state penalties and settlement fines when breaches occur. Let's look at a few recent data breaches and see what happened, as well as what could have been done differently to mitigate risk.

Breach #1 - Community Health Systems

About the Attack:

In August 2014, Community Health Systems (CHS) suffered a criminal cyberattack that affected 4.5 million individuals. This made it the second largest HIPAA breach ever reported at the time.

Cost of Breach:

It is estimated the breach will cost Community Health Systems approximately $100 million.

What Happened:

The attacker, believed to be a state actor, bypassed security measures and implemented malware to copy and transfer data out of the company. The Heartbleed bug contributed to the vulnerability of the data.

What Could Have Been Done Differently:

ClearDATA's Chief Privacy and Security Officer, Chris Bowen said of the breach, "There are some attacks that are very sophisticated, very targeted, but the bulk of them are providers or payers missing the basic checklist of things they need to be doing." Having a HIPAA compliant, HITRUST-certified Business Associate could have helped Community Health Systems avoid this breach.

"It is becoming more and more evident in this digital age that data security breaches are inevitable," said Matt Ferrari, chief technology officer, ClearDATA. "However, the overall impact of those breaches can be substantially reduced with the proper planning, including an active monitoring program. In this case, once the attackers gained access, an active monitoring system could have alerted CHS to the issue and a patch could have been utilized immediately. Too often, organizations wait to patch, exposing themselves to massive breaches that could have been lessened, if not completely avoided, with the proper precautions in place."

Breach #2 - Anthem, Inc.

About the Attack:

In 2015 Anthem Inc., one of the world's largest health insurance companies, was hacked in a sophisticated breach that compromised the records of about 79 million people.

Cost of Breach:

Anthem Inc. has agreed to pay $115 million to settle a class-action lawsuit in June of 2017.

What Happened:

According to this report in Fortune, Anthem said in February 2015 that an unknown hacker had accessed a database containing personal information, including names, birthdays, social security numbers, addresses, emails, employment, and income information. This hacker had used common social engineering techniques to obtain the credentials of an authorized database administrator to extract one of the largest health data sets in history. Only after an alert employee noted a suspicious SQL query was the hack discovered.

What Could Have Been Done Differently:

Although the breach was the result of an employee opening a phishing email, with the proper data security

assessment and subsequent safeguards, such as multi-factor authentication, email threat filtering, more granular data isolation and micro-services strategies, the breach may have been prevented," said Chris Bowen. But not all safeguards come from technology. ClearDATA's Chief Technology Officer Matt Ferrari adds, "This is why creating a culture of compliance within your organization is so important, so that all employees can help protect themselves, your organization and your clients."

Breach #3 - Advocate Medical Group

About the Attack:

According to a 2016 story in the Chicago Tribune, four unencrypted laptops with the personal health information of approximately 4 million people were stolen from an Advocate administrative office in Park Ridge. Later that year, two additional breaches followed, including theft of another unencrypted laptop.

Cost of Breach:

After several years of litigation, Advocate Medical Group was fined $5.5 million dollars in a settlement reached in August of 2016.

What Happened:

The breach compromised the electronic health information of more than 4 million people. The settlement stated Advocate had failed to provide sufficient risk analysis and management to ensure electronic health information was secure. The Chicago Tribune reported, "HHS' Office for Civil Rights investigated the breaches and found that Advocate failed to properly assess the risks related to the data. It also found Advocate didn't reasonably safeguard a laptop left in an unlocked vehicle overnight, and it didn't adequately limit access to its information systems."

What Could Have Been Done Differently:

"Quite often I see organizations who encrypt data at rest, but forget data in motion," said Chris Bowen. In addition, the proliferation of mobile devices, including laptops, tablets, and smartphones has made encryption and overall security more difficult to manage. "In order to adequately protect sensitive data, encryption should include data in use, in transit, and at rest," said Bowen. Cloud access to data would have helped mitigate this breach because the sensitive PHI would be viewed through a secured browser connection rather than being stored on mobile devices that could be lost or stolen.

The Costs Exceed the Fines

It's important to acknowledge that in addition to these staggering fines in the millions of dollars, other punitive costs are incurred in data breaches. "On top of the fines, organizations may have to pay $8-$12 a month, per person affected, for credit recovery services," said Matt Ferrari. "The forensics team to investigate the breach, the attorneys, the security experts needed to implement remediation, all would have cost less in advance of a breach than after. Just the notification of first-class mail to millions is a considerable add-on expense. But some of the greatest expense is in business interruption and ultimately business loss, not to mention litigation fees."

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. Top healthcare professionals trust ClearDATA's HIPAA-compliant cloud computing platform and infrastructure to store, manage, protect and share their patient data and critical applications.