Codify
BY AAPC

Health Information Compliance Alert

Data Security: Are You Ready for the High Price of a Data Breach?

Caution: Annual report ranks healthcare as hackers' top target.

Try as you might to prevent them, cyberattacks still happen - and the financial and professional consequences can be substantial. With data breach costs skyrocketing, it's crucial to put a plan in action to minimize your risks.

Background: IBM, in coordination with the Ponemon Institute, released the annual "Cost of a Data Breach Report," and the news isn't pretty. The 2021 results were compiled from research on 537 organizations of various sizes across 17 industries in 17 different countries. Data breach costs increased between 2020 to 2021 by a record 10 percent, the biggest spike in seven years, indicates the report. "Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the history of this report," IBM says.

But, that's not the worst news. For the eleventh straight year, healthcare experienced the hardest hit from hackers. The average cost for a healthcare data breach swelled to more than $9.2 million in 2021, a whopping 29.5 percent increase from the previous year, the report says.

"Compromised credentials" accounted for 20 percent of the data breaches studied, while ransomware attacks that maliciously destroyed data cost victims more than other types of incidents. Coming in at around $4.62 million per breach, ransomware assaults were actually costlier than the median amount for all data breaches at $4.2 million, the report asserts.

Remember: "Ransomware is a virtual stick-up," warns attorney **Steven Richard** with Nixon Peabody LLP in Providence, Rhode Island. "Hackers essentially try to find the weakest links in your system to be able to take your data, hold it hostage, and make you pay a ransom to be able to obtain and use it in the future."

"Unsuspecting workers will click on a link or an email and consequently infect your system with encryption that prevents access," Richard says. "Hackers typically target the most data-dependent businesses, such as healthcare or governmental functions, where the data has the most value and the ransom can be the most threatening."

Remote Work Bumps Up the 2021 Stats

Not only has COVID-19 made it more challenging for organizations to do their work, but it has also put them at a greater risk for data breaches. In fact, statistics from the HHS Office for Civil Rights (OCR) breach portal for the first seven months of 2021 confirm that HIPAA breaches are trending up, and impacted covered entities (CEs) and their business associates (BAs) are reeling from a boom of IT/hacking incidents (see Health Information Compliance Alert, Vol. 21, No. 7).

Why? If you're wondering why the numbers spiraled upwards in 2021, the quick move to remote work may be to blame, the report suggests. In order to keep work flowing, many businesses allowed their employees to work virtually. But that change happened swiftly, and many practices weren't technically equipped for that paradigm shift.

"Most healthcare organizations were completely unprepared to work from home securely when the pandemic hit," explains **Jen Stone**, MCIS, CISSP, CISA, QSA, principal security analyst with Security Metrics in Orem, Utah. "Most made valiant attempts to make do with what they had, engaging in an emergency mode that probably wasn't prepared for extensive remote work."

Virtual work-related breach costs were $1 million higher than standard issues. Additionally, statistics showed that the more employees a firm had working from home, the higher the costs of the data breach. When 81 to 100 percent of an organization's workforce operated remotely, "the average cost of a data breach was $5.54 million, or $1.30 million more than the overall average of $4.24 million, a cost difference of 26.6 percent," the report maintains.

Here Are the Implementations That Reduced Breach Costs

IBM looked at several factors that helped businesses reduce their breach risks and financial tolls. For example, the report investigates the impact of "Zero Trust" security architecture on breach costs, which assumes that any cybersecurity infiltration is possible and utilizes artificial intelligence (AI) and analysis to target issues.

"The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses," says the National Security Agency (NSA) in a fact sheet on Zero Trust models. "The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."

Though only 35 percent of the report participants employed a partial or fully realized Zero Trust model, those in a "mature stage of deployment" had a breach average at $3.28 million, $1.76 million lower than those not implementing Zero Trust security, IBM points out.

According to the report, other compliance tools that offered extra protection in tandem with Zero Trust models included the following:

- **Encryption:** The use of "high standard encryption" helped decrease organizations' costs by more than 29 percent.
- **AI and automation:** In 2021, firms that used AI and security automation to uncover data breaches mitigated their costs substantially. "Organizations with no security automation experienced breach costs of $6.71 million on average in 2021, vs. $2.90 million on average at organizations with fully deployed security automation," the report says.
- **Analytics:** Costs were 32.9 percent lower when analytics were utilized.
- **System complexity:** High level system complexity actually bumped up breach costs at an average of more than $5 million, "compared to $3.03 million at organizations with low levels of system complexity," IBM says.

Bottom line: Whether your organization is a small physician practice or a large hospital system, it's important to invest in data security. A HIPAA risk assessment can help you mitigate current and future risks, protecting both your patients and your wallet.

"Healthcare has traditionally been less sophisticated when it comes to information security … [but] now is the time to get serious about protecting systems, because lives and institutions are at stake," notes HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont.

Resource: Find the IBM/Ponemon Institute 2021 study at www.ibm.com/security/data-breach and review the NSA guidance on Zero Trust security architecture at https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.