Savannah Rude

RTV3305

04/24/26

From Corporations to Consumers: The Growing Threat of Data Breaches

A University of Maryland study found that, on average, a Fortune 500 company experiences an attempted data breach every 39 seconds.

Data breaches are becoming increasingly common, with an estimated 166 million individuals affected by one in the first half of 2025, according to the Identity Theft Resource Center.

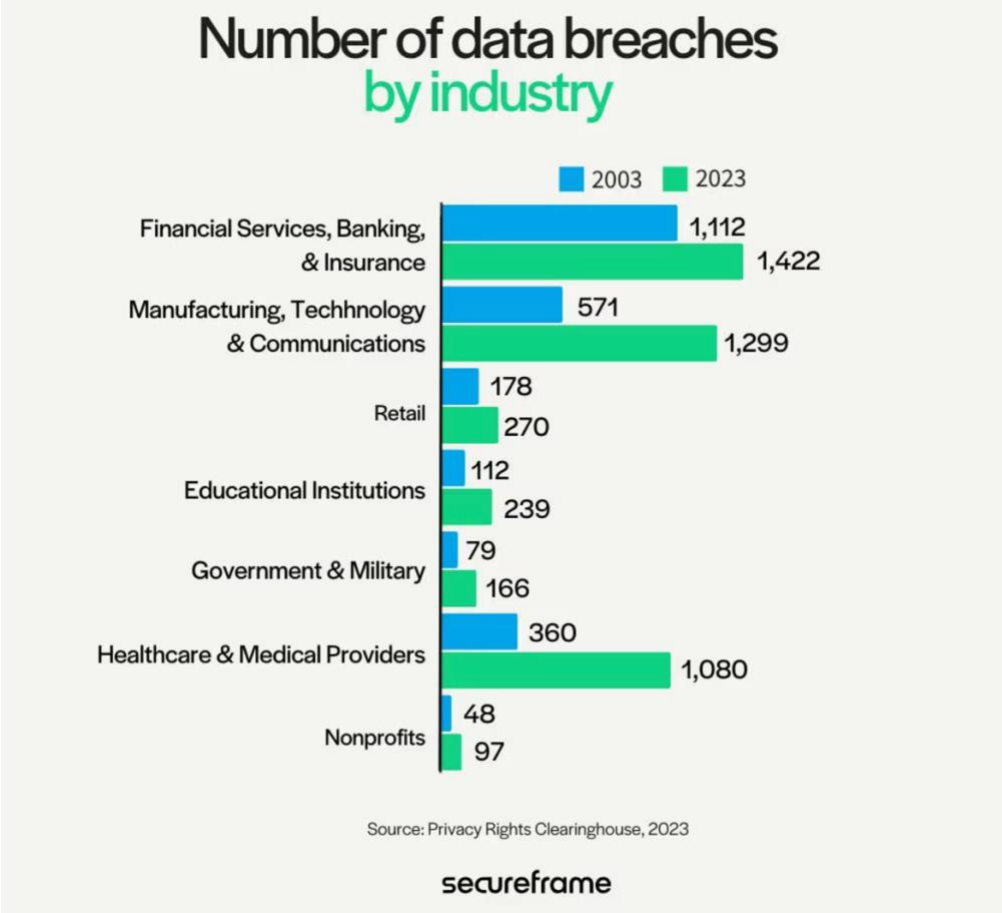
A data breach occurs when confidential, sensitive, or protected data is accessed, stolen, or disclosed by unauthorized individuals. These breaches can occur in many ways.

David Reeves is the Chief Information Security Officer for a third of the United States Army National Guard, which is about 500,000 people. He deals with data breaches daily.

Data breaches can happen at the corporate, personal and even national security levels, he said.

“A data breach is someone who has nefarious intent accessing controlled data for some sort of malicious intent,” Reeves said. “Whether or not it’s to change the data so that it could benefit them, steal the data for intellectual property theft or potentially state secrets that could cause national implications.”

In 2025, there were over 3,100 reported data compromises in the U.S. affecting over 1.35 billion individuals, according to Statista.



Courtesy of Secureframe

The graph above shows the industries most affected by data breaches, with financial services, banking and insurance, manufacturing, technology, communications and healthcare and medical providers reporting the highest numbers.

Data breaches can cause hackers to gain access to citizens' personal information from hacking companies within these various industries, Reeves said.

"Target had a very large data breach a few years back, and they (hackers) were able to pull information from Target's corporation's point of sales," Reeves said. "So, everyone who bought something at Target over a period of time, all of those people's information was stolen."

Not only can this affect the people whose information was stolen, but it can also cause large implications for organizations like Target, he said.

“The first one is obviously financial damage because if you have a data breach within your organization, you first and foremost have to respond to the data breach,” Reeves said. “So you’re paying people to come in and do forensics, to look up what was stolen, verify that it was stolen and verify that nothing else was affected.”

Large organizations will also typically offer to pay for credit monitoring for any affected individuals, which adds to the financial burden. Some organizations, like Target, have to shut down their businesses for a certain period, which can greatly increase the financial burden, Reeves said.

Besides large corporations like Target, data breaches can commonly happen in the medical field.

Zoe Leitner, an operational assistant at a healthcare consulting company, serves on a compliance committee and works to protect patient information during data breaches. She said that, in the medical field, it is less likely that such incidents personally affect individuals whose data has been leaked.

“A lot of times when that data is hacked, especially when it has to deal with patient information, the hackers will essentially hold it for ransom,” Leitner said. “Companies are never supposed to pay the ransom, so at that point the hackers can’t do anything with the information, so not that it doesn’t matter, but it shouldn’t specifically affect you.”

Leitner said that medical companies should always use the highest level of encryption when handling patient information, and that patient information should never be sent over email.

One impact of data breaches seen across all industries is reputational loss, Reeves said.

“It’s the harder part to measure as far as impacts to an organization because it’s not a pure math thing,” Reeves said. “The rest of the stuff you can quantify relatively easily, but capturing

how someone loses trust in an organization is harder to capture because it's more of a qualitative measure, not a quantitative measure."

A lot of times, data breaches come down to education. Reeves said that many times, organizations are not as informed about the risk of a data breach and choose not to spend money on certain security tools because they believe a data breach won't happen to them.

"From a cognitive perspective, if you said, 'Hey, if your organization could end up losing $5 million because of a data breach, or you could prevent the data breach for $1 million,' that's a pretty simple math problem," Reeves said. "But the paradox there is that a lot of times organizations decided to say 'No, we won't do that, because it won't happen.'"

Hannah Blanton, a student at the University of Florida, had her identity stolen in 2023 due to a data breach.

Blanton said she started noticing strange charges on her credit card at various places in California. It wasn't until her mom contacted the credit card company that she realized her identity had been stolen, too.

She said she had to have multiple meetings with the IRS to have her Social Security reinstated and her identity restored.

"I felt really violated, and it was honestly frustrating because of all these steps I had to take just because of a data breach," Blanton said.

After this experience, Blanton said she is much more aware of where she puts her personal information.

"I'm definitely more cautious about apps that I put my credit card information on or where I keep certain passwords and stuff," Blanton said. "I make sure not to keep some of that

stuff written down on my phone, and I'm more cautious with the places I'm using my information at and cookies and stuff like that."

Leitner said that having cyber awareness is very important and that it is especially important to verify links online before clicking them.

"A lot of practices are using AI texting, so just make sure you don't click anything suspicious and make sure it's from the practice," Leitner said. "You obviously couldn't cause a whole breach, but it could cause a breach of your information if you're putting your date of birth, contact information and Social Security on a website that isn't real."

Reeves said his biggest recommendation is for people to always ensure their phones and laptops are up to date and that their credit is locked.

Anyone can log into each credit bureau and lock their credit for free. Reeves said it is extremely easy to lock and unlock as needed and is one of the best things an individual can do because, if personal data is swept up in a data breach, the credit bureau will prevent a hacker from using it and notify the individual.

"It takes like 10 minutes to do, and it really isn't hard at all, people just don't know it's there," Reeves said. "It's astounding when you think about it because we use credit in so many different aspects of our lives."

If you suspect that you have been a victim of a data breach, change your passwords, freeze your credit, monitor your financial statements and report it immediately to the Federal Trade Commission.

Sources:

Hannah Blanton

850-687-9730

David Reeves

9045367851

Zoe Leitner

561-578-1082