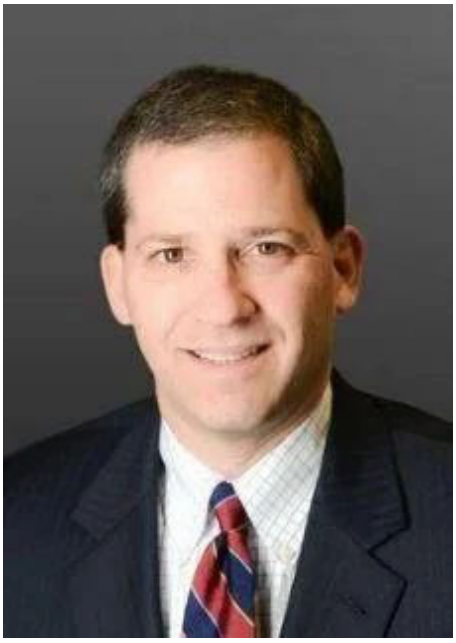
https://www.clevelandjewishnews.com/features/special_sections/legal_affairs/data-breaches-can-include-identity-theft-loss-of-assets/article_d352353c-ecc9-11ec-9398-5fdbd12bc252.html

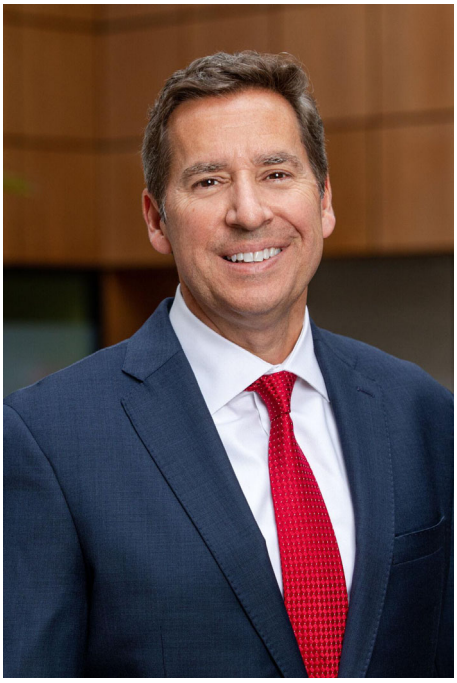
Data breaches can include identity theft, loss of assets

MEGHAN WALSH
mwalsh@cjn.org
Jun 15, 2022



Stovsky

Meghan Walsh



Giszczak

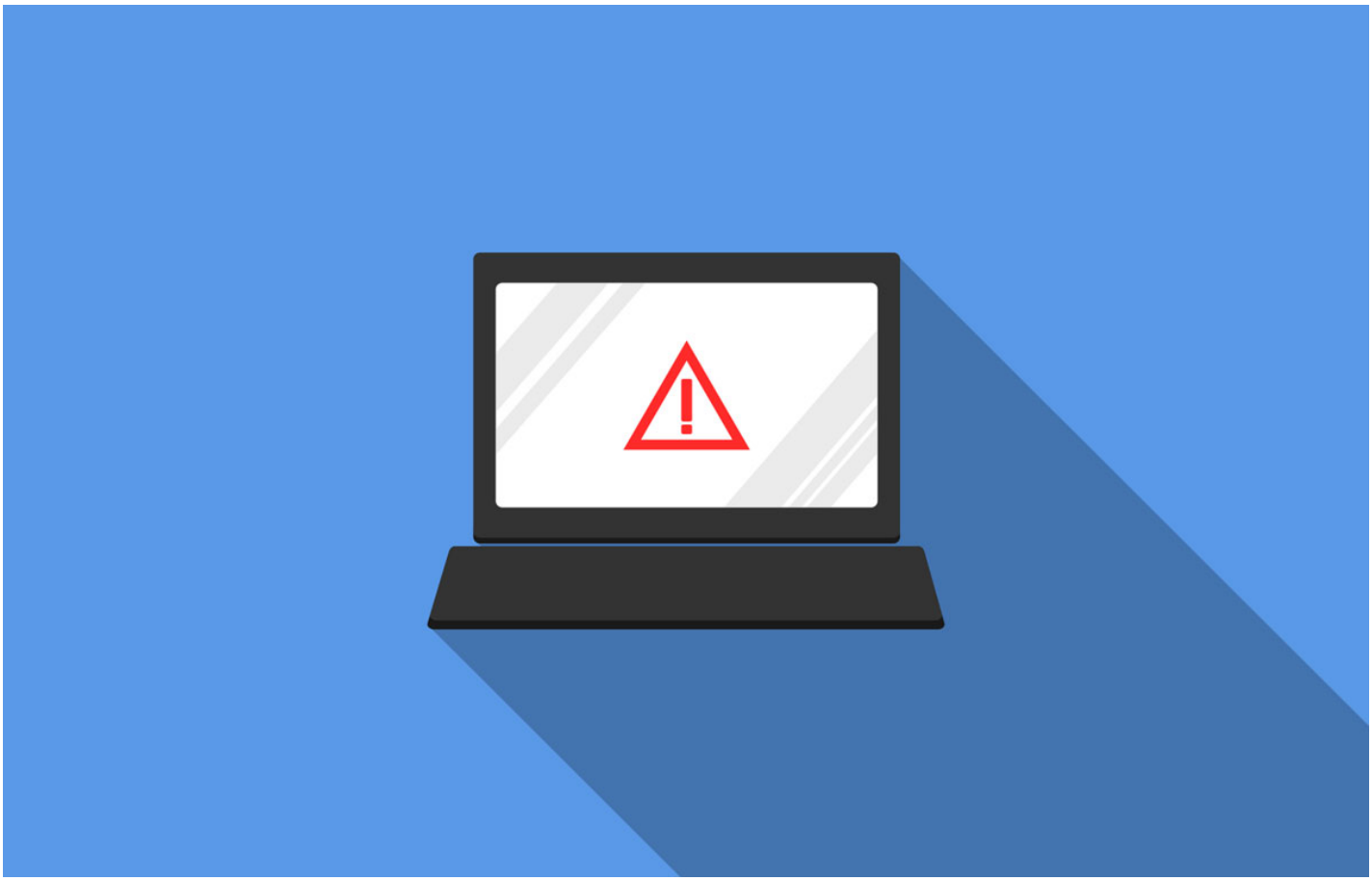


Image by Darwin Laganzon from Pixabay

These days, it is impossible to avoid the storage of our personal information on computers. Many institutions that we depend on in order to live have systems that hold our addresses, telephone numbers, dates of birth and Social Security numbers in computers and on the internet.

Crooks around the world spend the majority of their time trying to hack into these systems. When these breaches occur, our information becomes at risk. Consequences of breaches include identity theft and significant loss of financial assets.

Jim Giszczak, chair of litigation department and co-chair of data privacy cyber security practice group at McDonald Hopkins Law Firm in Cleveland; and Michael Stovsky, partner and chair of the intellectual property and technology practice at Benesch, Friedlander, Coplan & Arnonoff in Cleveland, spoke about what causes these breaches and how companies who host the systems should respond.

In most instances, human error causes security breaches, Giszczak explained.

“It’s oftentimes somebody that gets phished,” he noted. “They give up their credentials, they click on an email they shouldn’t click on. Sometimes, it’s just a vulnerability with a system or a piece of software that gets exploited, but the vast majority are just the result of human error.”

Giszczak said the leading causes of data breaches are ransomware, business email compromises and wire fraud.

“With ransomware, the criminals get, essentially, access to your systems and they start to encrypt them and they demand a payment in order to provide you with the encryption key,” Giszczak said.

He went on to say that, with wire fraud, a criminal gets into someone's email account and impersonates another individual that they know. The criminals wait for the appropriate time when a large payment is to be made and move emails between legitimate users to a spot where they will not be seen by them, he added.

"Then what happens is they will then send out a fraudulent email with fraudulent wire instructions, instructing whoever is making the payment to make it to a fraudulent account," Giszczak said.

After this, attorneys often see disputes over who is responsible for the lost money, he added.

In responding to these events, Giszczak recommended that the liable parties reach out to insurance brokers to find out if they have coverage for the loss and reach out to legal experts so the investigation is covered by attorney-client privilege.

Stovsky said that liability may fall on the company whose system was compromised, a third-party contractor who was hired to service the system or a criminal who invaded the system.

He explained that, in the case of it being a company or contractor error, they may enter into a settlement, by verbal agreement or by litigation, with the affected parties.

"We do see litigation in the data breach area so sometimes parties that have liability won't admit it (and) they have to be sued," Stovsky said, adding that, in this case, such action may be taken to force the responsible party to make reparations for the error.

In the case of criminal activity, the "bad actors" may be held liable and subject to prosecution, Stovsky stated.

When searching for an attorney to assist in these legal proceedings, Stovsky said the three most important elements to look for are experience in the field, knowledge of the topic and trustworthiness.

“I think it’s important to find a lawyer that works in this area and doesn’t dabble in it, that works in this area full time and it’s what they do.” Stovsky noted.

Meghan Walsh