

“The short answer is, if you have a breach, your first call should be to your attorney, because you want them running the response to have the privilege in place.”

- Eric Levine

The legal response

So, you have a breach? Or you think you might have a breach? Or you want to check to see how vulnerable you are to a breach?

Then, your first call should go to ... your lawyer.

That’s right, before bringing in security consultants for an analysis or talking to your team, you should get your attorney involved.

So said **Eric Levine**, co-chair of the cybersecurity and data privacy group at law firm **Lindabury, McCormick, Estabrook & Cooper**.

“To protect any small business, you need to have legal involved, if for no other reasons than to cloak what you are doing with privilege or confidentiality — by that, I mean communications with your attorney that nobody else can get to,” he said.

Levine, speaking at the NJBIZ Cybersecurity conference held last week at the **Raritan Valley Country Club** in Bridgewater, explained how companies can get hurt by doing the right thing when it comes to cybersecurity.

“Think about it,” he told the audience. “You hire (an expert) who comes in and does a vulnerability assessment and they find out you have a gaping hole in your security. That’s great. You fix it.

“What if you don’t get the fix in before there’s a breach and all of your employees’ information gets put out on the net and people have identity theft? One of your employees loses everything and they come back and say, ‘I’m suing you because you were



Eric Levine, co-chair, cybersecurity and data privacy group, Lindabury, McCormick, Estabrook & Cooper.

- ANDREW MILLER/FOR NJBIZ

negligent in keeping your system secure.’

“What’s the best piece of evidence that they are going to have that you were negligent? The analysis that you just did, which showed the gaping hole in your security. So, you say to yourself, ‘What did I just do? I hurt my company by doing the assessment.’”

That’s why, Levine said, you bring in a lawyer from the start.

“You hire an attorney and your attorney helps you do your critical analysis; we run that assessment for you,” he said. “The results of that assessment are now privileged, which means the outside entity that wants to come after you can’t get to it. Because, as

the attorney, I asked for it to give the advice.”

Levine was pressed on the issue. There was a suggestion that with increased requirements for cyber, such a conversation would be open to discovery.

Levine said he’ll fight the fight.

“Where there’s a regulation that says, ‘You have to provide this information to the entity you are doing business with,’ I’m still going to argue that when the third party comes and tries to sue me, that regulation does not apply to them, so they are not entitled to that information.

“There is not a lot of case law yet that says that privilege will be pierced, but there

is decades of case law on privilege that protect me.”

Levine detailed when companies, by law, have to report breaches. He said any breach where personally identifiable information is accessed by someone who is unauthorized (first and last name plus a Social Security number or credit card information) has to be reported to the state police.

“You have no choice,” he said. “You have to do it.”

Of course, like any lawyer, Levine said there are grey areas.

“You could have a breach that does not rise to the level of a reportable offense in New Jersey,” he said.

And while companies can over-report, he said, there are reasons for being out front and transparent.

“There are plenty of companies out there that have given notifications that they don’t need to, to basically say, ‘Just so you know, we’ve had a cyber-intrusion. It’s been contained, but here’s what you might want to consider doing: Change your password on our site or do X, Y or Z.’”

The alternative is worse.

“There’s an issue in transparency in cybersecurity that you need to be aware of,” he said. “If you hide something like this, it will come back to haunt you.”

That’s why – well, you know where this is going.

“The short answer is, if you have a breach, your first call should be to your attorney, because you want them running the response to have the privilege in place.”