Interview Issue

Cyber crime fighter

Levine says companies can't be too prepared for a cyber breach — or they could pay a steep price

BY MEG FRY
mfry@roi-nj.com

Companies across the globe today are under constant threat of cyberattack.

That issue alone keeps **Eric B. Levine** rather busy.

"Cyber was one of the newer practice areas we strategically looked at (this time last year) when considering our future," said Levine, the executive vice president and co-chair of the Cybersecurity and Data Privacy Group at the law firm **Lindabury, McCormick, Estabrook & Cooper** in Westfield.

"We knew that there would be an increased need for counsel for clients dealing with issues such as data breaches and related litigation, including the negotiation of cyber insurance policies and drafting of cyber policies and procedures for firms."

After graduating from **Seton Hall University** School of Law, Levine completed a clerkship with the Superior Court in Essex County before joining Lindabury, McCormick, Estabrook & Cooper in 1996 to focus on commercial litigation and business disputes. The firm, which started in 1954, had grown from its focus on mom-and-pop businesses to also serving the larger middle-market and some Fortune 100 firms.

But size doesn't matter when it comes to cybersecurity, Levine said.

More than half of all cyberattacks are directed at small and midsized businesses, costing those organizations an average of $1.8 million in losses and costs to restore normal operations.

And those figures do not consider the 60 percent of companies who go out of business within six months of a cyberattack.

ROI-NJ recently spoke with Levine to learn what businesses should do before and after a data breach.

Here is some of that conversation:

ROI-NJ: *What is the No. 1 thing that New Jersey businesses need to understand about cybersecurity today?*

Eric Levine: No matter how big or small your business, cybersecurity affects you. Companies need to anticipate that they will be a victim at some point, if they are not already. There are two types of companies out there: those that have been breached and those that have but just don't know it. There could be a virus in your network now that you have no idea is there.

Some people seem to think that because their business is small or because they aren't a certain type of business, like a technology company or a multinational, that no one is looking to hack into their information and steal their client and employee data. That is just not true. Whether you are a local bakery or a global pharmaceuticals company, you have to take these things seriously.

If you do not address (this issue) and you bury your head in the sand, chances are, if and when you are confronted with a data breach, you will be woefully unprepared. Statistics will tell you that small- and medium-sized businesses that are unprepared for cyberbreaches tend not to survive them. The cost of responding to, correcting and closing any data gaps, as well as protecting your business' reputation, can easily cost millions of dollars. Therefore, every business, no matter how big or small, must have a cyber or data privacy component within any sort of operational plan that they have.

Eric B. Levine's work as co-chair of the Cybersecurity and Data Privacy Group at Lindabury, McCormick, Estabrook & Cooper is keeping him busy. — *MICHAEL EIN*

ROI: *What is the first thing a business should do when it discovers a cyber breach?*

EL: While it depends on the actual type of breach, whether it be a phishing attack, industrial espionage or so on, the same things tend to apply. For example, if you are hit with ransomware, such as when someone infects your computer with malicious software that locks up your information, you will need to decide how you will respond to the ransom demand. Will you pay it, or will you hire professionals to help you break the code and retrieve the information?

If you have purchased a cyber insurance policy, you should call your carrier to dispatch someone to help you. If not, one of the first things you should do is to call an attorney who handles data breaches and let them run the response for you. If there is a lawsuit by an employee or vendor regarding someone's information that you have allowed to be disclosed, you don't want the results of your investigation being used against you in trial. The attorney will then get in touch with the appropriate people to detect the problem, contain it, analyze it, determine how to close the gaps and provide notification.

There is no single federal law that governs data breach notification in the U.S. There are 48 states that have unique laws governing this, including New Jersey, where there are very strict guidelines as to when and how you should provide notification to the people who may have been harmed. In New Jersey, for example, you should not provide notice of a data breach until you are given approval to do so by the state police. If you discover a data breach, one of the first things you should do after you contact your attorney is to contact and report it to the New Jersey state police and the division of public safety. They will then investigate and give you the go ahead as to when you can provide such notification.

ROI: *It seems like there is a new breach every day — has this changed the way that businesses think about the type of information that they require vendors or clients to provide?*

EL: I think we do have to change the way we think about that, yes. For example, people used to use their Social Security numbers for everything. But they were never meant to be identifiers for people to buy things; they were for governmental purposes only. Perhaps we as a society should reconsider that.

I mean, think about it — when you purchase anything from a store today, they ask for your phone number, and you readily give it to them. But the stark reality of it is, there is a subset of humanity out there trying to get that information. That is all they do. Whether it is a student in a dorm room who just wants to cause trouble, a crime syndicate in Europe trying to take your money or a state-sponsored agency trying to disrupt the government, they are all out there and they all want different forms of information. There's no reason to think that this will ever stop, because they have been successful. I don't know that the age of privacy is dead, but you certainly do have to take a lot more steps now to protect it.

ROI: *When there is a federal investigation going on into possible cyber breaches of the U.S. government by foreign countries, I mean, how can businesses even begin to keep their information secret?*

EL: If someone wants to get at your information and you do business or connect with people online, you are vulnerable. If you are the one company that doesn't do any of that — maybe you're old school and you order all your stuff over the phone — congratulations! Because, for companies today, a data breach is all but inevitable. So, now, what companies need to figure out is what kind of information that they have which could be of value to someone else, and the reasonable steps they can take to protect it.

You can invest in firewalls, antivirus software, encryption, etc., to make you safer than you once were. But statistics state that the No. 1 cause of data breaches is still human nature.

ROI: *Give us examples of how companies can be fooled?*

EL: Someone may call you up, say they met you last week at a conference and they'd like to come to your office to meet with you. They say they're going to get there a bit early and they're wondering if it'd be possible for you to give them your office's Wi-Fi password so they can just go online without having to bother you. You might give them the password and potential access to your entire Wi-Fi network, even though it turns out that caller is sitting in the parking lot outside of your building and never planned on coming in.

Or a hacker might take a flash drive loaded with malicious software and drop it in that same parking lot for someone to pick up and say, 'This must be someone's from the office.' How do they find out? They plug it into a computer to see what the files say and unknowingly upload that malicious software.

This is the human element that needs to be dealt with through continuous training. We need to keep telling people not to click on that email with a link from someone they don't know or from a client that they weren't expecting. A little bit of diligence can go a long way.

ROI: *How else can you protect your information?*

EL: Even though you may know what kind of valuable information you have, and you've trained your employees, you need to constantly back everything up and purchase cyber insurance. It's also important that if there is a breach, you act quickly. You may not be able to stop the spread of private information if someone does breach your data, but you can at least notify people that their information was taken so they can take steps on their own to try to prevent any damage, such as freezing their credit, checking their credit reports and purchasing a credit monitoring service.

CONTINUED ON PAGE 20

Interview Issue

CONTINUED FROM PAGE 19

ROI: *How much is this sort of thing costing U.S. businesses?*

EL: There is no easy answer to all of this but any answer that is out there requires significant capital investment. You have to be willing to put money into it to protect yourself by installing patches, making sure your software and firewalls are up to date and that your servers are secure. Then, you also should consider getting a cyber insurance policy. They're not as expensive as people think they are and the prices are coming down. Even if you get just $1 million worth of coverage, while that may not be enough to 100 percent cover the cost of a cyber breach for a small- or medium-sized company, could you imagine if you didn't have it at all? One of the things that seems to be lost on people is that, if you have a cyber breach and you must respond, at the same time, you still have a business to run. How are you going to deal with both?

That is why businesses also should establish policies and protocols that govern how they do business. A good example is the protocol we have for dealing with outgoing wire transfers. We get things sent to us in writing and we call and verify the address before we send out any money to ensure we are not wiring money to a fake address. We represented a pair of doctors from Manhattan last year who got caught in that sort of scam and wired $750,000 to purchase a home to a fake bank account. They got a call a couple of hours after the closing that the seller had not yet received the money. They immediately panicked, called us, we got on the phone with the bank to say we think that there's been a scam, and we were able to freeze all the money before it was distributed because the hackers were not as sophisticated as they might have been and did not transfer the money as soon as it hit the account. That could have been worse.

ROI: *What sort of cybersecurity issues are on the horizon that are not yet widely known?*

EL: The good news is that things are out there and are constantly being reported. The **New Jersey Cybersecurity and Communications Information Cell** sends out a weekly email blast to anyone that is a member to bring them up to speed on things that are going on. They identify new types of hacks, new phishing or spam techniques — what we've seen a lot lately are deviations of the old types of issues. For example, people don't expect to get text messages with embedded links, but that's something that is happening quite frequently. I ironically got one while I was teaching a seminar on cyber-training, a text message from a company that I had never done business with a link for whatever the reward was. Or, perhaps you're still getting robocalls from computerized voices saying they're calling from the **IRS**, but, now, hackers are running programs so that the number that comes up on your phone has the same area code and the first three digits as your phone number, which psychologists will tell you that when someone sees something familiar like that, they drop their guard and they pick up the call.

People need to protect themselves from what can happen. For example, we are going to be feeling the implications of the **Equifax** breach for years to come. Smart hackers won't jump on it right now when everyone is looking — they are waiting for people to get complacent. In the wake of a breach, something may raise a red flag for you, but six months from now, it may not. … I took the calculated approach of assuming that I was part of that breach, froze all my credit and subscribed to **Lifelock**. Because, by the time you get a credit report that tells you there have been unauthorized requests for your information, the damage is often done.

ROI: *Anything else?*

EL: Not only do we need to be a little more careful than we used to be, but we also need to slow down. That is really understated these days. We're moving so quickly because we want to respond at the speed of light. Everybody needs to slow down, take a breath, and look at things before we do them. That alone can go a long way in minimizing the likelihood that you will be a victim of a cyberattack.

twitter: @megfry3