BUSINESS FIRST

Don't have a good cybersecurity plan in place? Then don't plan on getting a lot of business in the future

The response after the latest ransomware attack has become standard. Or you could call it cliché.

For the most part, New Jersey companies were spared from the **WannaCry** cyberattack that produced more than 200,000 incidents in more than 150 countries last week.


Tom Bergeron

But it had many business executives around the state scrambling to get info experts said they should already have had: details of their company's cybersecurity program.

And then, after their companies were spared, many offered the same old lines about how they know the next attack is coming and they need to devote more resources to protect their businesses going forward.

But the expert panelists at the **NJBIZ Cybersecurity conference**, held last week at the **Raritan Valley Country Club** in Bridgewater, said cybersecurity plans are as much about gaining future business as they are about protecting what you have.

If you're the thought leader and decision-maker in your company, here's the biggest takeaway: What's in your cybersecurity protocols and — more importantly — how seriously you take them, may be as vital to your business development as anything else.

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

Levine said cyber-protocols already are making a huge impact in heavily regulated industries. He thinks it's just a matter of time before they are standard in all.

"How many people work in a regulated industry like health care or banking?" he asked the audience. "How many people work with governmental agencies? Anybody bid on public contracts? Guess what's going to be a requirement in the future for you to get a public contract? They are going to want to see your cybersecurity protocols in place. It's going to happen."

It's already happening.

"If you're a related entity to a health care provider, you're going to have to have certain things in place for you to win the contracts," Levine said. "They're going to say, 'Show us your data protocols.'"

Those protocols, he said, apply to all the companies you do business with. The protocols of any contractors, freelancers or consultants you hire are just as important, Levine said, pointing out the infamous Target breach is believed to have been started through an HVAC contractor.

Ignoring protocols — or just paying them lip service — is no longer an option, our experts said.

"You can choose not to, but best of luck to you," Levine said. "You'll be exposed to liability and you're going to miss business opportunities. The question is a very telling one. It's really going to guide how we do business in the future."

Peter Bamber makes it his business to make sure other businesses have protocols that are up to speed.

Bamber, a vice president at **Information Security Consulting Services**, said that means having a team in place — a team that knows its roles and has practiced its roles — before an incident.

"What we see constantly when we respond to these incidents and breaches is that we walk into a building and they'll have us sit in a room with 15 people for hours discussing (the incident)," he said.


From right, panelist Peter Bamber, vice president, Information Security Consulting Services, shares his thoughts while joined by fellow panelists Eric Levine, co-chair cybersecurity and data privacy group, Lindabury, McCormick, Estabrook & Cooper, and Hal Soden Jr., insurance and risk management advisor, Oliver L.E. Soden Agency, during the NJBIZ Cybersecurity conference at Raritan Valley Country Club in Bridgewater. - ANDREW MILLER

Three takeaways

One final word from each of the panelists at the NJBIZ Cybersecurity conference held last week at the **Raritan Valley Country Club** in Bridgewater.

Hal Soden, insurance and risk management adviser, Oliver L.E. Soden Agency:

"Even with all the employee training and guiding your employees to make sure you are adhering to (all security protocols), you still can't prevent everything. Sometimes, it's the people who know the most that make the mistakes. Just think of **John Podesta**. His job was basically to advise on security matters, and he fell for the scheme of changing his Gmail password and you saw what happened there. Skilled people can make mistakes."

Peter Bamber, vice president of Information Security Consulting Services:

"As part of the training, I always ask how many people have smartphones and, of course, everyone raises their hands. So, I ask them, 'Why are you conducting personal business on a business system? Why are you endangering your business system by looking at **Facebook** or tying your business email address to **UPS** packages?' These are situations that lend themselves to phishing and compromising your systems. The takeaway I always give is to get people to stop conducting personal business on those business systems. Yet — at the same time — the business should be putting as much technology as possible in place to protect them from themselves."

Eric Levine, co-chair of the cybersecurity and data privacy group at Lindabury, McCormick, Estabrook & Cooper:

"Take a holistic approach. Educate your employees. Take the steps to assess the vulnerabilities, act on those steps. Use privilege to protect yourself, even when doing an analysis. Cloak yourself in confidentially so people can't use your own evaluation against you."

"And then they'll say, 'Let's get to work.' And there's three hours left to do the work or you're working all night. And then you have more meetings the next day, instead of having teams of people working on getting everything under control."

Bamber said the key is working from the start.

"The incident response team should have a group that sits at the meeting and determines a course of action," he said. "They go out and get that information for the people doing the work and then come back and report on their progress.

"Maybe there's an end-of-the-day wrapup, but let the people do their jobs. You can save thousands or millions of dollars, potentially, if you have a team."

Defining that team — before the breach — is key, Bamber said.

"Who is that team?" he said. "You may have dozens of outside vendors that you are working with and you're going to bring in people like us. Do you have a documents? Have you identified every single person who should be involved in it and who is allowed to communicate? Who is allowed to communicate to the outside? That should all be defined as part of that program."

Of course, part of that team is your insurance representative.

Hal Soden Jr., an insurance and risk management adviser at **Oliver L.E. Soden Agency**, said the cyber insurance sector is changing on a daily basis.

You could hear it in how he described his actions after the WannaCry attack.

"A couple years ago, I would have said (companies) should have considered purchasing cyber liability insurance along with risk management items and asked about the employee training they should have been doing," he said.

"Now, my concern is whether the insurance that they have is adequate for what their risk is. Insurance has transformed, advanced and made a lot of changes. So have the risks. What keeps me up is not if my clients have insurance, but whether it will address what's happening."

The cyber insurance sector has become so specialized, companies need to clearly understand the extent of their coverage. Or potential lack of coverage.

"I'm sure there are plenty of people out there who feel they have cyber insurance because it's included in their business owner's policy," Soden said. "Hopefully, most people know that it's not included automatically in their general liability. It never really was.

"In 2004, the insurance service organization slapped an exclusion on the standard general liability policy. For about 10 years, we've had standalone cyber policies. The last couple of years, companies are adding some endorsements, where you can add this coverage back, but usually it's subject to some sort of limit."

"I'm sure there are plenty of people out there who feel they have cyber insurance because it's included in their business owner's policy. Hopefully, most people know that it's not included automatically in their general liability."

- Hal Soden Jr.

How does a typical policy handle a reply to a ransom?

Soden said many policies won't cover that.

"There just isn't a standard yet," he said. "It's more common for it to be included in coverage but it's something that you should have never assume."

One thing is clear: If you are not doing things policies ask you to do — have plans, have teams, practice protocols and, most importantly, apply security patches as soon as they are available — your coverage may amount to nothing.

Soden said policies won't cover you, "if you're supposed to be doing things and you're not."

Moving forward, Levine said, cyber protocol plans are key.

"Everybody should have a cyber response plan," he said. "You have your disaster plan. Everyone remembers Superstorm Sandy, we all knew who to call for our insurance, who to call for our backup files, etc.

"You need to have a plan for cyber up front. You need to establish protocols. Do you have a 'bring your own device to work' policy? Can you bring your own personal laptop and connect it to the system? You need to lay these things out. You need to do your own vulnerability assessment or an ethical hack. Hire someone to come in and figure out where you are vulnerable."

And then share the information.

"You need to educate your employees," Levine said. "You need to tell them, 'Here's what to do, here's what not to do.' And do it often. It's like your cyber fire drill."

How many companies are doing this? Not nearly enough, Bamber said.

When asked to grade the companies he sees, few are anywhere near the honor roll.

"You would have to be a very successful regulated business to be a 'B+,'" he said. "Everybody else is no higher than a 'C-,' and there are a lot lower than that."

Cyber grades matter. Soon, they will mean business.

— Tom Bergeron