ROI-NJ Thought Leadership Series: Cybersecurity

Why bring lawyers in

Attorney-client privilege can be crucial for businesses' protection

It's just common sense to bring in legal counsel if a company suffers a cybersecurity breach.

But here's something many small business owners and company executives don't realize: By that point, it may be too late.

Bob Anderson, shareholder at **Lindabury, McCormick, Estabrook & Cooper** and an expert in cybersecurity matters, said counsel needs to be brought in to oversee all cybersecurity planning and preparation for one simple reason: attorney-client privilege.

If you have a breach and your company gets sued — and it will, Anderson said — having all of your preparation protected could result in huge savings of both money and reputation.

Anderson, speaking at a recent ROI-NJ Thought Leadership Series panel, explained how.

"When you're first starting to put together a program to protect your company, one of the things that you will typically want to do is hire someone called an ethical hacker, who will try to get into your system," he said.

"The results of this kind of a penetration testing that determines the vulnerabilities and weaknesses in your system will be in a report that goes on for pages and pages of all the problems in your system. If you do end up with an attack and end up in litigation, Exhibit A in the litigation is going to be this detailed report that shows all the vulnerabilities of your system, and they'll be able to see how you elected to prioritize the problems.

"The litigants are then going to say you knew you had these vulnerabilities and spot the one you didn't fix."

Having legal counsel order the penetration test would likely shield that document by virtue of attorney-client privilege, Anderson said.

"If they are hiring it on your behalf and in order to provide you with legal advice, then that report is potentially protected by attorney-client privilege — and it can't be used against you."

Anderson said this attorney-client privilege would pay off after an attack is discovered, too.

"Similarly, if you actually do have an attack, it's sort of counterintuitive

that one of the first people you would want to call as your attorney," he said. "But, if you call your attorney first and get them involved from the very beginning and you're gathering information in connection with them so that they can advise you on to how to comply with the law in order to address the issues that have come up in this attack, then again, much of what you're doing can be shielded by attorney-client privilege."

"I can't say that this is absolutely perfect, that it will never allow the information to be disclosed, but it can potentially provide you with protections."

Most of all, Anderson said, it brings stability to an unstable situation.

"When an attack first happens, everybody's panicking, everybody's running around with their heads in the clouds and trying to come up with a plan and not everything is done sensibly," he said. "But, if it's done in a way that you're still working toward getting answers to comply with the law, then that consultation is potentially protected.

"It's one area that people almost never think about in terms of cybersecurity, but it can potentially be one of the best things you could possibly do to help limit your liability in those situations."

Bob Anderson, shareholder at Lindabury, McCormick, Estabrook & Cooper and an expert in cybersecurity matters. — *THOMAS P. HUGHES*