# CYBER BREACH RESPONSIBILTY

Cyber security has progressed past the voluntary stage with Federal and state cyber security regulations. Initially the regulations focused on the financial services and health care industries due to the sensitive information they keep.

Recently, the regulations expanded to include businesses in every industry and have become more specific about what constitutes proper cyber protections.

Yet, some companies consider cyber regulations as a burden and a "box to check." To counter this, regulators are becoming stricter in enforcing compliance and imposing fines.

While no one likes paying fines there is another price to pay for failing to take proper precautions, losing the trust of your customers, clients, or patients. They came to you for your knowledge and skills but also trust you with their personal and private information.

Cyber breaches occur, everyone is getting used to that. But what if your protections are deemed inadequate, or worse, negligent? Will trust be lost? If so, will your business survive?

The American Bar Association, ABA, recognizes this and issued Formal Opinion 47 which states:
"[A] lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

Special security precautions are defined his way:
"The opinion lists seven factors to consider when determining the appropriate level of cybersecurity: the nature of the threat; how client confidential info is stored and sent; the use of reasonable electronic security measures; how electronic communications should be protected; the need to label client information as privileged and confidential; the need to train lawyers and nonlawyer assistants, and the need to conduct due diligence on vendors who provide technology services."

Despite this, the industry report from 2020 showed how few law firms followed these precautions. Only:

- 43% of respondents use file encryption,
- 39% use email encryption,
- 26% use whole/full disk encryption.
- 39% use two-factor authentication
- 29% use intrusion prevention
- 29% use intrusion detection (29%)
- 28% use remote device management and wiping
- 27% use device recovery
- 26% use web filtering
- 23% use employee monitoring and,
- 12% use biometric login

# CYBER BREACH RESPONSIBILTY

While this is specific to law firms and the ABA, evidence suggests that the cyber security requirements and the lack of compliance is not substantially different in other industries.

If you are not implementing proper cyber security precautions, you may be putting your firm at risk for a cyber breach. The result may be fines. But failing to take adequate precautions may result in a loss of trust from your clients/patients. Your business may be able to afford the fine, but will it survive a loss of trust?

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.