



AIS Network Cybersecurity Attorney Consulting Services

Why would cybersecurity attorneys consider using a team of cybersecurity engineers to consult for them?

Overview

In today's technological world, the business executives who are your clients likely understand the need to assess their company's cybersecurity risk and exchange information within the company to address that risk. As counsel, you may even have had to respond to and mitigate actual breach situations for that client, including the complex communications and coordination between various parts of the client's company.

Yet, there are legitimate business concerns about how the disclosure of that information might look in a litigation discovery proceeding.

The client's internal communications regarding weaknesses in the company's cybersecurity program may expose that company to greater danger in breach litigation. Also, policy development by IT and security personnel with no legal training may inadvertently expose the company to risk.

So what's the best way to handle that situation?



Managing Risk

Involving legal counsel in all important aspects of cybersecurity risk assessment and breach response is critical for the potential protection of the company under the doctrine of attorney-client privilege.

While clearly there are benefits in a post-breach, incident response scenario, there's also a strong case to be made for establishing these legal privileges prior to any incident.

AIS Network Partners With Cybersecurity Attorneys

AISN Partners With Cybersecurity Attorneys

AISN's cybersecurity team partners with attorneys in cybersecurity and IT practices at law firms.

We maintain a staff of highly-skilled and vetted cybersecurity engineers, who are capable of assessing a client's cybersecurity program and security maturity.

We then work with the client's attorney to design, implement and maintain a roadmap of specific initiatives that will preserve a reasonable and acceptable level of risk for the client.

Preserving Attorney-Client Privilege

For a client to preserve attorney-client privilege in the context of cybersecurity assessments and compliance, the ideal engagement involves the client retaining counsel to provide cybersecurity compliance guidance.

Counsel then retains AISN as a subject-matter expert and technical advisor.

In coordination with the client, counsel directs AISN's efforts, receives our reports and recommendations and then maps the results to the client's legal obligations.

Why Retain a Cybersecurity Consultant?

Many attorneys who retain cybersecurity experts to work with clients believe the decision is a no-brainer. The depth and breadth of knowledge that these professionals offer are invaluable to case outcomes.



Examples of AISN's services include:

- Identify strengths and weaknesses in the design and implementation of your current cybersecurity program.
- Develop and drive implementation of a roadmap of key initiatives to close gaps, build on existing strengths and correct program weaknesses.
- Lead the development and update of cybersecurity policies, procedures, standards and guidelines, leveraging our subject-matter expertise on best practices applicable to your business environment.
- Guide the establishment or improvement of your vulnerability management program, including regular vulnerability assessment and remediation activities.
- Oversee incident response planning and breach investigation activities.
- Help you ensure that your cybersecurity program complies with legal, regulatory and contractual requirements
- Provide third-party cybersecurity assessment and auditing services, including risk assessment, cybersecurity audits, vulnerability assessment and penetration testing.

Interested in learning more about how we can support your law firm? Contact us today!

P: 847.202.1400 | E: sales@aisn.net | www.aisn.net