Cybersecurity Questions for Major Stakeholders

Questions for Internal Stakeholders…

Do you have cyber liability insurance in place for your company and any subsidiaries?

What major corporate stakeholders are responsible for cybersecurity efforts of the organization?

Do you outsource IT or security functions, or do you have the expertise to handle internally?

What experience does your existing IT team have in handling security incidents?

Have you identified external sources of expertise to call on in the event of a security incident? (i.e. legal resources, PR, forensic support, insurance etc.)

Have you developed an incident response plan so that your company knows how to handle a security incident if one occurs?

If you do have an incident response plan, has it been tested?

Have you ever had a third party perform some type of Cyber Risk Assessment or Audit?

If so, what framework was it aligned to, what were the results and when was the last time it was done?

Are you familiar with the ISO/IEC 27000 family of information security management systems, or other similar frameworks?

Do you feel that your employees are properly trained to identify and avoid potential security incidents?

In the context of a client contract, what liabilities do you have in the event of a security incident?

Questions External Stakeholders…

Do you include cyber liability insurance requirements in contracts with your suppliers?

In the context of supplier contracts, how are your suppliers held liable in the event of a security compromise?

If you happen to outsource IT functions, when was the last time that you reviewed your contract with them?

Have you catalogued external systems or applications that may have access to your network?

For any suppliers that might have access to your network, do you use exercise the principle of least privilege and separation of duties?

For any suppliers that may require access to your physical or networked assets, is such access managed and protected?