Rapid CyberRisk Assessment

To assist board members and an organization's senior leaders in determining if they have latent cyber risk issues within their organization, I have developed the following questionnaire to allow non-technical leaders to rapidly assess whether there are indications of serious shortcomings.

This questionnaire is based on the Gramm-Leach-Bliley Act (GLBA), established in 1999, which specified the legal requirements for the protection of consumer information. A component of this legislation, called the Safeguards Rule, specified minimum safeguards for the protection of consumer information and was amended in 2021 to encompass the following 9 foundational elements of all security programs.

Based on these elements, I have developed a concise list of questions which can be used to quickly assess whether their information security program and organization is at least meeting these foundational requirements. As such it should be considered a dashboard warning light of potential problems, and is not intended to replicate the results of an in-depth cybersecurity assessment.

To use this questionnaire, consider for each question whether the requirement has been fully met (including whether it is documented), partially met (may be done but not documented, or done inconsistently), or not done or not met. Those elements which are not done or met should be considered the areas of highest risk, those that are partially met as being the next level of risk, and those that are met as being the lowest risk. From this prioritization, action plans should be developed to address these risks.

1. Designate a Qualified Individual to implement and supervise your company's information security program.

1. Has a person been designated as being responsible for developing, implementing and monitoring the organization's information security program.
2. Does the designated person report to the CEO, Board or a non IT leader?
3. Does the designated person have demonstrated experience leading and managing cybersecurity programs and teams?

2. Conduct a risk assessment.

1. Is there a documented risk assessment policy and process in place?
2. Is a cyber risk assessment conducted at least annually?
3. Does the cyber risk assessment consider the most likely threats to the organization's key assets, and the organization's readiness to counter these threats?
4. Does the cyber risk assessment produce prioritized recommendations to implement/strengthen the organization's controls to counter the identified threats?

3. Design and implement safeguards to control the risks identified through your risk assessment.

1. Are the organization's implemented safeguards traceable back to the organization's risk assessment?
2. Are the organization's safeguards aligned to a recognized security standard such as those from the Center for Internet Security (CIS), the National Institute of Science and Technology (NIST) or an industry required standard?
3. Is there a high level information security policy, approved by the board, that specifies the safeguard requirements?
4. Are the standards, procedures and operational requirements for the safeguards documented and reviewed at least annually?

4. Regularly monitor and test the effectiveness of your safeguards.

1. Are the safeguards monitored on a regular basis to ensure that they are meeting their mandated requirements?
2. Are the safeguards tested on a regular basis by an independent 3rd party to ensure their effectiveness?

3. If safeguards are not meeting their mandated requirements, is there a process in place to document and track required remedial actions?
4. Is the operational status of key safeguards and remedial actions reviewed on a regular basis with senior leadership?

5. Train your staff.

1. Are all staff trained on joining and at least annually thereafter as to the organization's information security policies and requirements?
2. Are all staff trained on threats and issues applicable to their roles (administrators, developers, etc)?
3. Are all staff tested on a regular basis to ensure that they are aware of key threats and how to respond to them?
4. Is the status of staff training and testing results reviewed with senior management on a regular basis?

6. Monitor your service providers.

1. Are service providers classified as to the risk that they pose to the organization, and are their contractual requirements aligned to that risk?
2. Are all service provider arrangements reviewed by security prior to contract signing for key contractual clauses and requirements?

3. Are service provider's required to meet security and data privacy requirements at least as stringent as those of the organization itself?
4. Are service providers required to inform the organization in the event of security incidents or an substantial change to the processing of the company's information?
5. Are service provider obligations and contracts reviewed on a regular basis, as specified by their risk rating?

7. Keep your information security program current.

1. Is the information security program documented and updated on at least an annual basis?
2. Does the program encompass at least all of the GLBA requirements, or other mandated requirements based on the company's industry including regulatory requirements?
3. Does the program include the risk assessment process and the key initiatives undertaken to address the latest risk findings?
4. Does the program include the security organization structure and functions, and how these align to the security policy requirements?

8. Create a written incident response plan.

1. Have documented incident response plans been created to address the most likely potential information security incidents?
2. Are these plans tested and updated with learnings on at least an annual basis?
3. Are there designated personnel responsible for the implementation, maintenance and testing of the company's incident response plans?
4. Have appropriate relationships been established with internal stakeholders and external resources needed for support and response in the event of an incident?

9. Require your Qualified Individual to report to your Board of Directors.

1. Does the designated security leader provide a written update to the board at least annually regarding the state of the information security program?
2. Does the written update provided encompass at least the following information: Status of the Information Security Program, Risk Assessment Results, Service Provider Arrangements, Results of Security Testing, Security Events or Violations and Management's Responses, Recommendations for

Changes in the Information Security Program, Associated Budget for the Information Security Program, Recommended Action Plan

3. Does the designated security leader have the authority to independently speak with the board's designated representatives responsible for cyber risk?

Once you have obtained the answers to the previous questions, use the results to develop an action plan, if needed, to address any areas where you determined that the answer was not fully met. To the extent that your assessment indicated multiple areas of deficiency, you should consider that an indication that there may be more serious areas of risk within your organization, and that you should consider engaging a professional to conduct a more thorough and in-depth review.