The Cyber Liability & Risk Assessment Review for Business Owners and Executives

("Lower Risk, Reduce Liability, Protect Reputation and Prepare for the Next Data Breach")

Listed here are actions you should take ASAP to ensure you have done your due diligence to lower the risk of a cyber-security incident or breach, to ensure all employees have a working knowledge of how to protect information, to ensure you have a solid incident response plan when a breach occurs, and to lower your potential liability and protect your reputation when a breach does occur. In a perfect world, this project should involve a representative from each section of the company, to include the company leadership, and MUST be driven from the Top. This is just a summary assessment to get you started and help put some pieces in place for your security program now while you plan and budget for a full security assessment/audit. Again, this assessment is just a start to help you understand what information you have and how it is or should be protected. For questions or issues you do not have an answer to, I encourage you to reach out to experts for help. Security is a process, not a "set and forget" concept. Don't let it overwhelm you. You can plan for and manage small pieces at a time. Remember, there is no clear definition of "reasonable security." As stated it is a process and in order to lower risk, reduce liability and protect reputation you must be able to show what actions you took to identify, address and react to various risks and threats. For corporate directors, "reasonable" is what makes sense for your company as long as you can provide a rational justification and that you made the effort to address. See due diligence and corporate judgement rule.

1. Do an Assessment –

It is important as a leader/manager or owner, that you understand what sensitive data your company possesses, where it resides and how it is protected. For a small organization this may appear to be an easy task. But, I encourage you to begin to map out where all data exists, even outside the organization where you do not necessarily have control other than maybe through the law or contractual obligations. For large organizations this will be quite an undertaking, so develop a process to begin incrementally, requesting information from each section or site. The pain will be worth the reward.

a. Make a list of all of the information your organization collects, processes and stores.
b. Categorize this information. E.g. public, confidential, secret, top secret, sensitive, etc.
c. Determine where/how information enters the organization and where/how it leaves (ingress/egress).
d. Next, determine who, within the organization, has access to which information and whether their access is required as part of their job?
e. Determine, who or what individuals/companies/vendors, external to your organization, have access to your network and/or the information on that network. (Remember, your network, as stated above, due to mobile devices, the Cloud, etc., extends far beyond the walls of the building.)
f. Now, investigate the state of your security. Determine how all information is secured, whether in transit or in storage. Obviously, the amount of security employed is equal to the level of sensitivity of the data. For many companies though, their security is applied equally to all information since it is more cost effective. Which model you use,

secure all or segment your security, will likely be determined in part after a cost-benefit analysis.

g. Determine how access to your network and information/data is controlled, for employees as well as outsiders.
h. Attempt to understand the points or areas where information exists, traverses or is stored, and security cannot be controlled or control is limited. This includes points within and outside of the organization. For instance, information on company or employee devices at their homes; information held or controlled by vendors, e.g. Cloud, attorney, accountant, managed services, etc.
i. Now, begin to list the known threats and risks to the information as well as vulnerabilities that may cause risks. E.g., potential theft of personal or financial information, insider theft, hackers, negligence/loss, etc. Once the known risks are listed, utilize those from outside your section or company to help you identify risks you may not have considered. These people may include someone to do a professional risk assessment, insurance adjustors who work with risk on a daily basis, searches on the Internet for common risks, etc. For example, additional risks to information may include competitors attempting to steal trade secrets, identify thieves trying to steal personal information like names, social security numbers, etc., or spammers trying to steal email addresses, and more.
j. Review the list of threats, vulnerabilities and risks and work from there. This is where you need to implement a risk management program to quantify and qualify each risk, do a risk-return analysis, determine what level of risk the company is willing to accept, and determine how to address each risk. In quantifying you will attempt to determine, using some sort of grading system (e.g. 1 to 5), the probability of a particular risk occurring. You should also qualify the risks, again, using a grading system, attempting to determine what impact a risk will have on the organization if it occurs. For example, a common risk is that an employee will click on an email and attachment introducing a virus to the network providing a foothold for hackers. Or, it could be, as is popular recently, a request appearing from a top executive, to transfer funds. Identify these risks, determine the level of likelihood, and what actions and resources are appropriate to assign to these risks.
k. Finally, once you have quantified and qualified the risks, threats and vulnerabilities, determine how you will address each: accept, mitigate, transfer or avoid/ignore. When you accept a risk, or other, you determine that it is more cost effective to accept than spend money to mitigate. You might determine that the risk is not high enough to be concerned with or the likelihood of it occurring is very small. When you mitigate a risk you take steps to lower or eliminate that risk. For instance, implement training, a policy and/or software to lower/remove that risk. Transferring risk may involve purchasing insurance to cover the risk or purchasing outsourced services so the risk then belongs to someone else. Avoiding, or ignoring the risk, which is not recommended, is doing nothing. In this case typically an assessment of the risk is not even accomplished.

2. Prepare a Message in Anticipation of a Breach –

Owners, CEO's, executives, managers, and others: what would you do and say if you found out tomorrow your organization was breached? Remember, most companies find out they have been breached from someone or an entity outside of the company. Normally you

+1-719-648-4176
david@titaninfosecuritygroup.com
www.titaninfosecuritygroup.com

will have very little time to react and to put out a statement once a breach is identified. When someone asks, comments from the leadership such as, “I don’t know, ask my IT guy or the IT company I hired,” will not instil confidence in anyone and may destroy your reputation, make you look incompetent, and cause your liability regarding the breach to soar through the roof.

a. When preparing a message in response to a potential data breach, think about what you would want to say if hacked. What can you say to convey that you did everything you could to prevent the breach, and, that you are taking control of the situation to fix things now. Also consider how what you say will help you protect the company reputation.
b. Once a breach occurs or a potential breach is identified, if you or anyone from the company is asked to or makes a statement, don’t admit to anything. It is likely, once you are notified of the breach or potential breach, that you have no idea what may have occurred, how much data was lost or stolen, if any, or impacted, etc.
c. When preparing your incident response plan, generate a few versions of the message you want to put out in the event of a breach, whether to media, board members, shareholders, clients or customers. These situations are usually fluid, so generally any prepared message will likely have to be modified depending on the facts. But, it is much better to be prepared and have a sense of what you will say versus trying to develop a statement as you are being pressured.
d. Remember, most breaches get worse when company executives make statements, typically unprepared, or they say nothing. If you are not sure what to do, find an expert who can help. Also, remember, whatever you put out in your message may be thrown back at you when you are put on the stand in a lawsuit.

3. Draft/review/implement the necessary policies –

The policy or policies you draft and implement inform employees and anyone handling company information what their responsibilities are and what is expected of them. The policy is also used to show that you have met any compliance issues, and, can be used to show customers/clients, or potential customers/clients and others your network is connected to, the steps you have taken to secure data. In some cases you may want to have internal policies just for employees, and one or more external policies that you can show to outsiders who ask about your security. This will ensure you are not revealing sensitive procedures about your security.

a. Do you have any policies related to protecting information/security? If yes, review them to determine which, if any help to lower or mitigate one or more of the risks on your list.
b. If you don’t have policies then they must be drafted. Ensure policies that are drafted are not done so in a vacuum. You may draft a policy with good intentions but not realize the additional requirements it puts on someone else complicated his or her job. A representative from each section should be involved in the drafting and certainly the review.
c. Each organization is different but all need a security policy, acceptable use policy, privacy policy, incident response policy and more. Some others that are common

+1-719-648-4176
david@titaninfosecuritygroup.com
www.titaninfosecuritygroup.com

include social media, encryption, password, backup, business continuity/disaster recovery, and many more.

d. Ensure that all policies take into account law or other regulatory compliance for the company and the industry or industries you operate in.
e. If not sure how to draft and implement policies then hire someone to do so. But, be careful, many companies will simply sell you a set of canned policies that are not tailored and customized to your organization and its particular situation. If limited in budget you can find policies online or purchase cheap policies and then customize for your organization.
f. All employees should sign the policies in order to create a record in the event something happens. Then, no one can claim he/she did not read or understand the policies.

4. Cyber-Security Awareness Training –

The end-user (this includes ALL in the company), in many cases, is the weakest link in your organization. We are all dealing with a lot of data almost every waking minute of the day, whether on a computer at work, at home or a mobile device on the go. It is far too easy to make a mistake or click on something not realizing the vulnerability it creates or the malware/virus that may be downloaded. Additionally, we frequently send emails to the wrong person out of haste, or send data we didn't mean to send. Training is the only way to help you and your workforce understand the threats, vulnerabilities, risks, who hackers are, how data is lost or stolen, and what employees can and need to do to protect the company as well as their own personal information.

a. Ensure all/everyone (the boss too), attends cyber-security awareness training at least annually. It is imperative that employees understand the threats to information, how it is lost or stolen, who is seeking to steal it and the methods used. If it has not been done in the past, cyber-security awareness training should be conducted immediately.
b. Implement a monthly cyber-security awareness program to keep employees fresh on the techniques they should be using as well as current threats.
c. After the policies are finalized this class should be repeated incorporating the requirements and responsibilities outlined in the new policies to emphasize why these requirements and responsibilities are important and how they are designed to help protect information.
d. A live cyber-security awareness class is preferable. Online and written courses are opportunities for employees to rush through. The live class will emphasize the seriousness and importance of protecting information.

***** Security is a process, not a "set and forget" concept. The above will provide you with some of the necessary tools to manage this process. In light of the speed at which breaches are occurring, I encourage you all to look into cyber insurance. Getting breached is no longer an "if," it is a "when" and "how often." You might as well use all the tools at your disposal to protect your company.

+1-719-648-4176
david@titaninfosecuritygroup.com
www.titaninfosecuritygroup.com

* The trend in the courts after a breach, is to look at the “reasonableness” of your security. There is not a one-size fits all or even a silver bullet to security. Cyber-security is a process of determining, based on threats, vulnerabilities, sensitivity of information, budget, workflow, organizational culture, and more, what works best for your organization, and then being able to defend that program or process. But you must first understand it.

“Never Ready, Always Prepared!”
(You can never be Ready for everything, but you can always be Prepared for anything.)

+1-719-648-4176
david@titaninfosecuritygroup.com
www.titaninfosecuritygroup.com