Your Security Risk Assessment: A Step-By-Step Guide

www.infinityinc.us

INFINITY

Your Security Risk Assessment: A Step-By-Step Guide

What is a Security Risk Assessment?

A security risk assessment is a process to help discover, correct, and prevent security problems within your network. It is much more involved than simply running a system scan to detect data security vulnerabilities and breaches, however. It is a complex process that should be performed by trained professionals who have experience assessing networks, identifying potential risks, and determining safeguard strategies.

A security risk assessment should be performed on a regular basis, such as annually. Every time a security risk assessment is performed, you should receive a risk assessment report. This should contain all of the details about the risk assessment process, what was scanned, and what was discovered. The findings might be positive or negative and should also include recommended actions.

Why is a Security Risk Assessment Important?

The general idea behind performing regular security risk assessments it to ensure that your network is working efficiently. Problems with your network will almost inevitably lead to disruption in day-to-day business operations. When your network is running smoothly, so will your business.

If you experience an attack by a hacker, network shutdowns, data theft, malware, worms or any other kind of security breach, your business will suffer, and this will ultimately affect your bottom line.

According to Avanan, 83% of people worldwide received phishing attacks in 2018, resulting in decreased productivity, loss of proprietary data, and damage to reputation. Over half of all phishing attacks contain malware, and 2 out of 3 phishing attempts use a malicious link. Clicking on the link typically installs malware or leads to a spoofed website where credentials can be collected. Most concerning of all is the fact that 25% of these phishing attacks breach existing security measures.

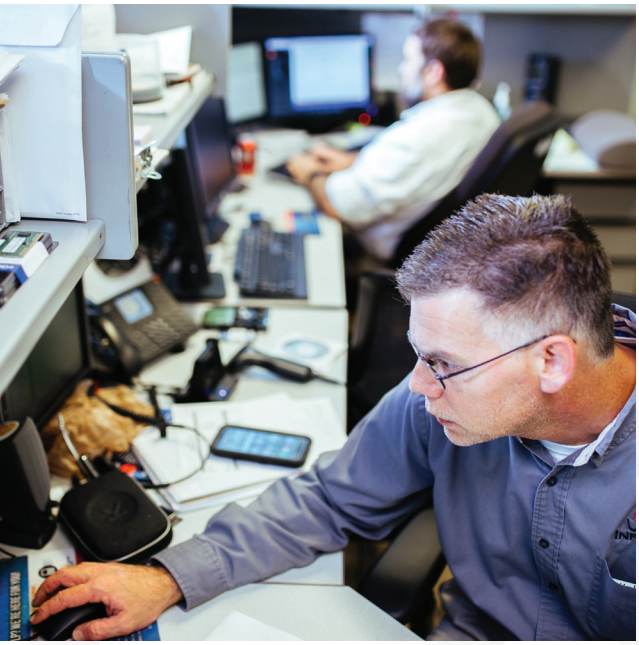
83%
of people worldwide received phishing attacks last year

1 in every 99
emails is a phishing attack

It is important to run security risk assessments consistently because technology is evolving every day and the current safeguards set in place to protect your network system can become impotent over time. By regularly checking your network system, you can upgrade your threat defenses to provide continuous protection from the most current threats.

HIPAA-affected Agencies

Any agency or firm that handles electronic protected health information (ePHI) is responsible for complying with HIPAA security requirements and regulations. HIPAA requires all businesses handling ePHI to analyze system risks, determine safeguards, and document the decision-making process throughout the system assessment.



"...you can upgrade your threat defenses to provide continuous protection from the most current threats."

Running security risk assessments and providing a risk assessment report are especially helpful. Not only will you ensure that your network system is safe, but you will be able to satisfy HIPAA requirements and show that your business is compliant.

Step-By-Step Guide

Step 1: Form a security risk assessment team

Before you can get started assessing your network system, you need to have a team of selected individuals in charge of conducting the assessment. Ideally, you will want to have at least one member from each department of your company to be on the team. You most certainly want to have a leading IT officer on board as well. Choose individuals who have decision-making power and have been with the company the longest.

"After you have formed your team and are ready to get started, the next step is to identify your system assets."

Step 2: Identify system assets

After you have formed your team and are ready to get started, the next step is to identify your system assets. What this means is that you need to identify the construction of your network, what its purpose is, what information is being stored, and how this information is used to benefit your company.

You also need to identify and sort the different types of information contained within your system (for example: patient records, social

security numbers, and credit card numbers). Then, identify where in the system the different types of information are stored.

In this step, you are essentially mapping out your entire network system and the information contained inside it.

Step 3: Identify existing or potential threats

For this step, you will want to create a threat probability model, such as a chart, that can be used to determine the highest risk areas in your network system. This step will probably take the longest amount of time to complete, but it is also likely to be the most important part of the assessment.

> "...you will be able to see other areas of your network system that may not necessarily be a high risk for threats, but a moderate risk"

Calculate the probability of threats based on the likelihood of different types of information being threatened. Consider how much of an impact a breach of these various types of information would have on the company.

Step 4: Determine safeguards and system modifications

Once you have determined your high threat areas, you can then determine what additional safeguards can be put in place to ensure that these sensitive areas are well protected. Based on your chart, you will be able to see other areas of your network system that may not necessarily be a high risk for threats, but a moderate risk.

Check to see what preventative measures are currently in place.

Step 5: Complete full risk assessment report

It is important to document the entire risk assessment process into a well-written report upon completion. You need to thoroughly detail each and every step of the process so that readers can easily see where the network system currently stands against threats. Risks and safeguards need to be explained along with how the team came to these conclusions.

Our Partnership

A risk assessment requires a thoughtful, methodical, and thorough approach. It is critical to see that all areas are covered to keep your business in good shape. Follow the steps outlined above to keep both your risk assessment and your business itself on the right path. If you'd like to consult with one of our security risk experts today, give Infinity Inc. a call.

INFINITY

10 Chatham Center South Dr.
Suite 300
Savannah, GA 31405

912-629-2426
info@infinityinc.us