AFFINITY IT GROUP

www.affinityitgroup.com

SECURITY RISK ASSESSMENT

RISKS FOUND DURING A SECURITY RISK ASSESSMENT

As a CEO, you must be able to prove to independent auditors that your company's IT network has effective security measures in place. The best way to prove this is to carry out regular security risk assessments.

Note that it's not enough to conduct a security risk assessment without taking action. IT security is an ongoing process. According to a study from CyberEdge, 52% of companies believe they will be hacked in the near future. New threats and vulnerabilities emerge daily. Security risk assessments should be carried out, therefore, at least once every two years to incorporate all new threats to IT systems.

The old days of erecting firewalls and running virus scans are long gone. There are so many emerging vulnerabilities and security threats that it's impossible to combat them with dated techniques. What's needed is a measured approach.

ASSESS YOUR DATA

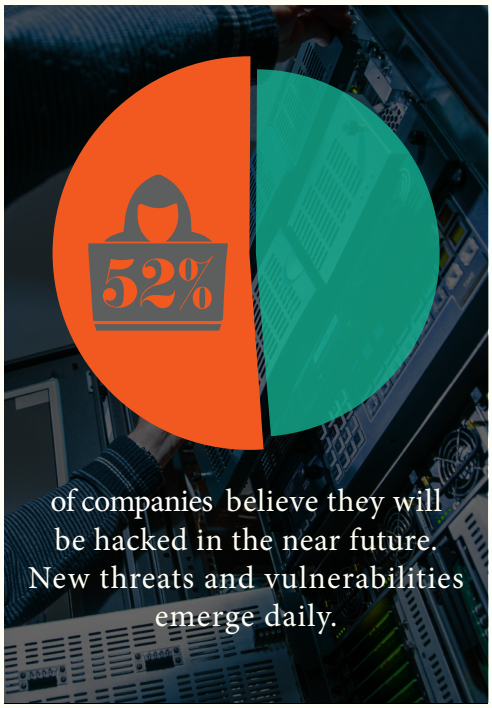
Assessing your data is the first step. This involves prioritizing which data should be protected most.

Ensure that critical data is protected foremost. Not all system vulnerabilities are a high risk. If the desire to exploit these vulnerabilities is low, then it's often more cost-effective to give them a low priority.

TYPES OF SECURITY RISK ASSESSMENT

Two types of assessment are usually carried out. One is an impact assessment, the other a likelihood assessment.

1. ***Impact Assessment***
   An impact assessment determines the potential harm a particular security threat can cause a company. The analysis is based on the



potential effect on revenues, cost, reputation, service levels, and compliance.

2. Likelihood Assessment

A likelihood assessment concerns itself more with the probability of a threat occurring. The more authorized users there are, usually the higher the risk. The risk also increases the longer a security threat is active.

TYPES OF SECURITY THREAT

Finally, it's important to categorize the different types of security threat. They can occur internally or externally, i.e., from someone working inside the organization or outside it.

Or, attacks can be malicious, i.e., criminal acts, or non-malicious, i.e., accidental. In fact, IBM's 2014 Cyber Security Intelligence Index states that 95% of all security incidents involve human error.

New system and software vulnerabilities arise daily. The most dangerous period for exploiting vulnerabilities is on the day new software is published.

A likely threat to mission-critical system data will register as a high impact threat to the organization.

A full security risk assessment can highlight many threats. Here are five of the most common.

1. Insecure Endpoints

Many employees nowadays are working remotely, using mobile devices to access the company's servers. Doing so may be convenient, but it also opens up potential vulnerabilities.

It's vital, but often unrecognized, that there is a secure entry and exit point to a company network. Cyber criminals are constantly probing company networks for the chance to infiltrate and steal data. It's important that there are no open ports and that corporate networks are protected from intrusion.

Protecting corporate networks in this way is known as endpoint security.

2. Cloud Encryption

Protecting your data from a cloud-based threat is best done using strong encryption at the data level, such as AES 256-bit. This is the gold standard in encryption. It is vital for protecting your most sensitive data. The crypto keys are kept safe by the data owner so that outside

parties cannot steal them. Unfortunately, not enough companies are encrypting their data in this way.

3. *Unpatched Software*

Most people understand that operating systems, such as Windows, need to be regularly updated. These updates include security patches that fix known vulnerabilities. If left unpatched, these holes risk exploitation by hackers.

Less well known are the vulnerabilities inherent within servers, routers, printers, and other devices. All require security patches from time to time. If these are not fixed, they can leave gaping holes in your network through which cyber criminals can steal your data.

4. *Password Protection*

Two-thirds of data breaches result from weak password protection. Would you use a two dollar padlock to secure your house? Too many small businesses are using weak passwords to secure their computer data.

Choosing simple passwords is bad enough When you're sharing those passwords with everyone in the office, you're looking for trouble.

Worse, routers and other hardware are often installed using vendor default passwords, such as 'admin.' This security flaw is a gift for cyber criminals who might be monitoring that company's network.

5. *File Sharing Protection*

Peer-to-peer file sharing applications can be useful, increasing work efficiency through enhanced collaboration. File sharing exposes your network to many threats, however, including malware and data redirection Information can also be stolen by unwarranted screen captures.

TRUST AFFINITY FOR YOUR SECURITY RISK ASSESSMENT

A security risk assessment will pinpoint all weaknesses in your company's network. These include the five most common security flaws listed above, but there are more! It's essential to run regular checks of your systems to spot vulnerabilities and rectify them before they result in malicious attacks or accidental damage. Affinity IT has the experience to run these checks and keep you protected. Let's talk about how we can protect you

AFFINITY
IT GROUP

www.affinityitgroup.com

Phone
+800.627.2214

Email
Info@AffinityITGroup.com

Address
6920 Spring Valley Dr
Suite 106
Holland, Ohio 43528