the NetWork

LeadingIT

Chicagoland CybersecurITy Support

September 2021

What's Your Cybersecurity Insurance Credit Score?

Insights On How Chicagoland Businesses Can Prepare For A Cyberattack

LeadingIT News

What's Your Cybersecurity Insurance Credit Score?

Insurance underwriters, as well as banking and financial institutions, extensively use credit ratings to estimate and manage risks. The higher your credit score, the lower your insurance and loan interest rates. With cybersecurity breaches and hacks at an all-time high, it is no surprise that insurance companies are now creating assessments to help them analyze the cyber risks of potential clients. In simple terms, insurance companies will now assess your cybersecurity posture to determine your insurance rates and policy terms. If the risk is too high, they can increase the rates or end your policy altogether.

Why Should You Care About Your Organization's Cybersecurity Score?

Nobody enjoys annual or quarterly visits to the doctor for wellness exams, but you make them anyway. It is an essential part of staying healthy. Regular checkups help you identify any early signs of illnesses and mitigate them before they become serious issues. Similarly, you take your car for regular multi-point checks and oil changes to ensure everything is okay to avoid getting stuck late at night in the middle of nowhere.

It's not any different when it comes to your technology environment. Proactive multi-point examination of your IT infrastructure to determine your cybersecurity score helps ensure everything is secure. Every modern-day organization should take cybersecurity scores seriously.

Here's why:

• Your cybersecurity score determines your insurance rates: As we said, cybersecurity insurance and other insurance companies are now keen on analyzing the cyber risks of potential customers. Higher credit scores will earn you more favorable policy terms and lower coverage costs. Conversely, lower cybersecurity scores will earn you higher premium costs, and in extreme cases, cancellation of your policy.

• Cybersecurity scores help you identify your cyber threat levels: The assessment process involves interrogating the cybersecurity protocols and systems you have in place. The subsequent score is a direct reflection of their effectiveness and weaknesses. It helps you understand your cybersecurity posture and identify areas that need adjustments.

• Cybersecurity score is essential in selecting your business partners: As you're doing your best to keep your company's systems and data safe, ensure that the organizations you do business with also make similar efforts. Otherwise, bad cyber actors can use them as backdoors to access your databases. And that's where a cybersecurity score comes in — your potential partners' ratings help you determine how well they are prepared to prevent and respond to hacks and breaches.

How Do Assessors Determine Your Cybersecurity Insurance Credit Score?

As is with most credit ratings, there's no standard procedure for determining cybersecurity credit scores. However, the following factors help assessors fully understand your cybersecurity posture, which is essentially the primary determinant of the ratings:

1. By Assessing Your IT Assets Inventory

You can only safeguard what you know. So, the first thing the cybersecurity credit score assessors will look for is whether you have proper visibility into all your IT infrastructure:

• Can you account for every on-premise, third-party, mobile, or cloud asset that is connected to your systems?

• Are they managed or not?

• Can you actively monitor their geographic locations?

• Are they core assets or internet-facing (perimeter) assets?

• How crucial is each asset to your business?

2. Through Checking Your Security Controls & Their Effectiveness

Cyberattacks begin as soon as hackers gain access to your systems. So, what protocols and systems do you have to keep them off, and how strong are these measures? Consider asking yourself the following questions:

• Do you have an effective password complexity and expiration protocol?

• Which intrusion detection and prevention systems do you have in place?

• Do you have an IT support team monitoring your network round-the-clock?

• Do you have a fast-response protocol if a breach occurs, and how often do you update it?

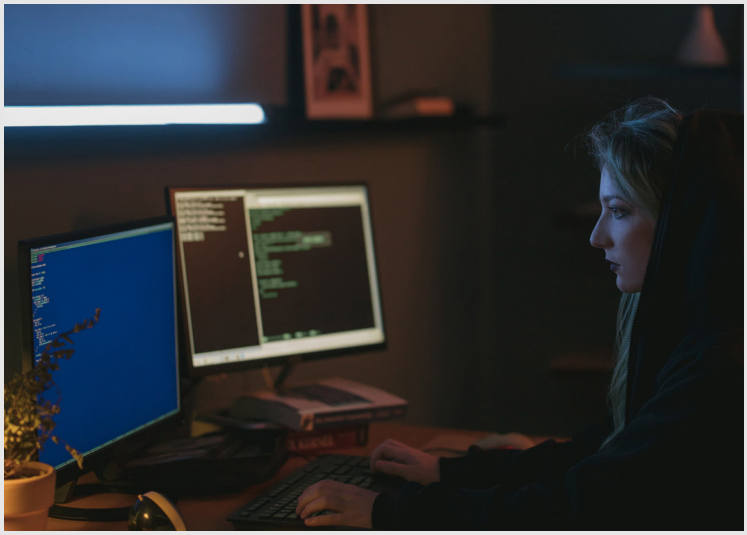
3. By Checking Your IT Support Team's Qualifications

Whether you're maintaining an in-house team or listing external cybersecurity service providers, how qualified are they? Do they have experience in working with organizations like yours?

The cybersecurity insurance credit score assessment team might also want to know if the IT support company has undergone any breaches before and how they handled it. For the best scores, you might want to work with a service provider with an impeccable reputation.

What's Your Staff's Cybersecurity Awareness Level?

Most data breaches result from employee negligence. Therefore, besides having solid protocols, you should also ensure that your staff is well-trained in detecting and preventing cybercrimes. Regularly train them on common cyber attack vectors and how to identify them. Cybersecurity awareness also entails your staff's preparedness to handle actual breaches. You might want to simulate attacks occasionally to measure their readiness levels.



Insights On How Chicagoland Businesses Can Prepare For A Cyberattack

Bad cyber actors are increasingly becoming organized criminals with well-structured techniques. This, and globalization, has made the fight against cybercrime more challenging than ever before. We are seeing an emergence of more and more nation-state cyber-terrorist groups targeting infrastructure from specific countries. Typically, they hack several organizations simultaneously and then demand very high ransoms. Hundreds of millions of cash in untraceable cryptocurrencies have been routed into these cyber-criminal terrorist gangs.

Why Can't Host Nations Stop These Cyber Terrorist Groups?

The answer is simple — they have no incentives to go after these crooks. And reasonably so — why would they trouble themselves going after cyber attackers who only target foreign companies when nobody is paying them to do so? Besides, the proceeds from these attacks usually go back to the home nations. So, even if the host countries don't shout it loud from the top of the mountains, they benefit from the hacks in one way or another. Therefore, the onus is on us to prevent these attacks. We must take a stand against global cyber-terrorism by investing in better infrastructure and implementing reliable intrusion detection and prevention mechanisms. Investing in these items will keep money out of terrorists' hands and put it back into our economy.

Why Is It Difficult To Trace The Ransom Paid To Global Cybercriminals?

Cybersecurity Ventures predicts that the global ransomware rates will jump to one per 11 seconds, with mitigation costs skyrocketing to over $20 billion by the end of this year. According to Sophos, U.S. organizations pay an average ransom of $170,104 and incur ransomware mitigation costs of approximately $1.85 million per attack. It's pretty clear from these figures that cybercrime is quite a lucrative venture. U.S. businesses and organizations lose billions of dollars to bad cyber actors every year. The question is — why can't the federal government trace these ransoms and bring the criminals to book? Well, there have been efforts by both local and federal cybersecurity agencies to track these terrorists and recover ransoms. Just last month, Deputy Attorney - General Lisa Monaco - confirmed the recovery of over $4.4 million that had been paid to hackers who took down the Colonial Pipeline's systems. While recovery efforts are not a new thing, most of them are usually not successful. That's because cyber criminals exclusively accept payments in cryptocurrencies which are almost impossible to trace. Again, hackers operate in the chaotic dark web where sites continuously rewrite their addresses, making it challenging to track them.

How To Keep Your Organization's Systems Safe

First, you have to assume that you are the next target. Nobody is safe. So, whatever cybersecurity measure you have, ensure that it's effective and up-to-date. While there's no protocol or IT support team that guarantees surefire protection against hacks and breaches, the buck stops with the basics:

1. Have strong passwords with a solid expiration protocol: Passwords are the most important and most vulnerable way of protecting your systems. Ensure that they are not only strong but also changed regularly. You should also have contingency measures like multifactor authentication and single-sign-on for scenarios where bad cyber actors steal your passcodes. of protecting your systems. Ensure that they are not only strong but also changed regularly.

You should also have contingency measures like multifactor authentication and single-sign-on for scenarios where bad cyber actors steal your passcodes.

2. Regularly assess your network: Sometimes, cyberattackers lay dormant in your systems for some time before launching an onslaught. They take this time to learn your systems, communication patterns, vulnerabilities, and how best to attack you. If you conduct regular assessments, you can identify the threats in your system early enough before they aggravate into severe breaches.

3. Deploy effective intrusion detection and prevention mechanisms: Even as you invest in keeping cybercriminals off your system, you cannot overlook the possibility of an intrusion. The earlier you identify intrusion attempts, the better.

4. Train your staff on cybersecurity: With several global cyber terror groups emerging by the day, your best shot at preventing hacks is to have cyber security-conscious employees. Regularly train them on the emerging threats, how to identify and prevent them, and fast-response protocols in a breach.

5. Maintain offline backups: Cyber attackers rely on confusion and urgency to coax their victims into paying ransoms. With your data encrypted, you might be tempted to pay ransom to resume normal operations. However, if you have offline backs of your critical files, you can sustain basic operations as you negotiate with the hacker or recover the data.

Should You Pay Ransom To Global Cyber Terrorists?

The issue of whether or not you should pay a ransom is a controversial one. One faction argues that no amount of money can salvage an organization's reputation or match the value of its data. The other argues that paying a ransom is like appreciating cyberattackers and encouraging them to launch more attacks. If you have a good backup plan you shouldn't need to pay the ransom. Enlist a cybersecurity focused IT company to ensure proper backups are in place to save your organization from debilitating ransomware payments.

LeadingIT News

Welcome Mallory (Office Manager) to the LeadingIT team!

As we continue to grow we are excited to add new positions to our business.

The staff was excited to show off their racing skills at K1 for our July community outing.