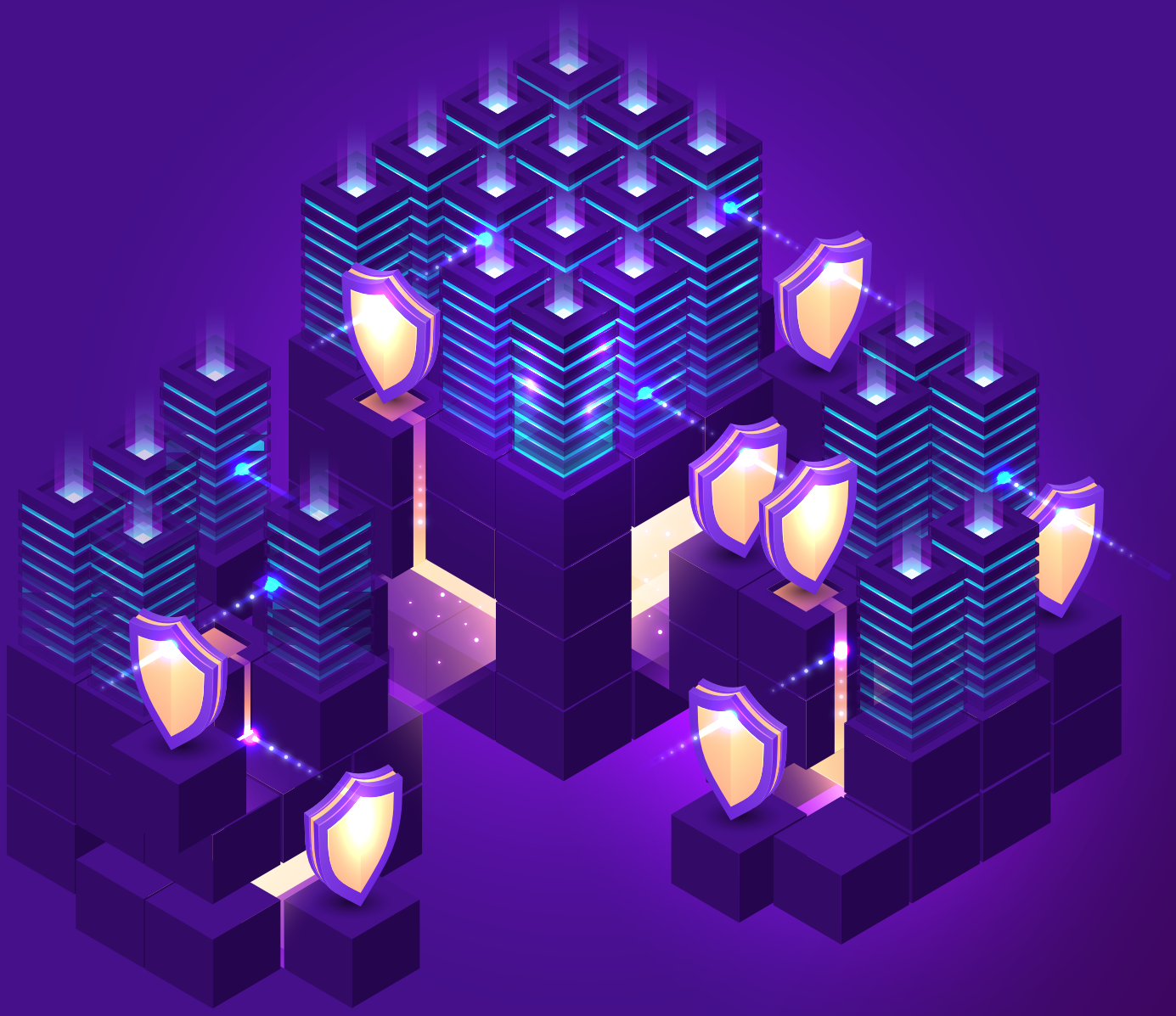
IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY

5 STEPS TO ASSESS AND **STRENGTHEN YOUR CYBERSECURITY POSTURE**

Cybersecurity is a complex and ever-changing landscape - so much so that every year, a new threat emerges. It's time for you to securely move forward with the help of these tips.

GET STARTED



www.ipsystems.ph

First, let's define what do we mean by **Cybersecurity Posture.**

This refers to your organization's collective effort to protect your sensitive data from cyber threats. This describes your overall defense mechanism - including your security policies in place, employee training, systems and applications, and more.

Being aware of your current cybersecurity posture empowers you to indentify potential weak spots, make improvements, and stay compliant to the latest industry guidelines.

Then, let's review our takeaways from 2020 - the year where cyber attacks became more rampant than ever.

- Sudden changes in the work environment is a perfect opportunity for threat actors.
- Employees are your first line of defense. However, they can also be the weakest link in your security strategy.
- Organizations that does not prioritize cybersecurity or make compromises in this area are the ones who suffer the most.
- Companies with immature security programs and rely solely on solutions are less able to deal with attacks when it occurs. Solutions and Training go hand-in-hand.

Therefore, what should we do next?

- Get smarter about optimizing investments and budget - ensuring risk is understood and managed.
- Cybersecurity planning needs to include remote workforce security.
- Cybersecurity training and certification for employees need to be prioritized.

Stay up to date on the latest cybersecurity news!

Follow us: /ipsystemsinc

IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY

Now, that you know some of the facts, it's time to take a look at your cybersecurity posture and lower the risks of attacks and breaches. **This how-to guide will help you.**

1 Follow a Security Framework

This will provide a strategic blueprint to help you stay safe. The most widely used framework us from the National Institute of Standards and Technology (NIST), and it has five elements which you can also apply in your organization. First, IDENTIFY potential risks, then PROTECT data by investing in the right technology, DETECT and monitor threats continually, RESPOND to breaches, and have a plan to swiftly RECOVER your systems.

2 Understand your Current Security Situation

It's vital to understand where your business is in terms of cybersecurity defenses. Carrying out a number of tests can give you a 360-degree view of your current strengths and uncover weaknesses. You can do different network tests but the most famous and reliable is doing Penetration Tests and Vulnerability Assessment.

3 Build Resilience

Once you have known your strengths and weaknesses, it's time to fortify defenses. Firewalls, Spam Filters, Antivirus Software, Employee Training, and more can take your cybersecurity to the next level. Adding more technology is also beneficial in filling security gaps, boosting efficiency, and automating processes.

4 Foster a Culture of Cybersecurity

Creating the right company culture and promoting education about security can help in significantly lowering the risk of breachers and phishing scams. This change involves awareness, testing, and training.

5 Plan for Cyber Attacks

Having an incident Response Plan will help you and your team know what to do when a threat infiltrates your system. This will minimize the risk of downtime, protect your reputation, and reduce the risk of losses.

Let's work on your cybersecurity posture. We can help!

CONTACT US:

IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY

+63 (2) 8638 - 3264

inquiry@ipsystems.ph

www.ipsystems.ph