https://datastrive.com

Datastrive

CYBER SECURITY

Your All-In-One Guide to Improving Your Security Posture

INTRODUCTION

Cybersecurity is a top priority for businesses across the world. Executives want to ensure that they're taking the proper steps to protect their data and their customers' data while staying out of the weekly data breach headlines.

After all, the last thing they want is to end up like Equifax, who leaked the information of 143 million Americans a few years back.

Or Marriott International, which let slip 20 GB of data affecting nearly 500 million guests.

In truth, it's essential for everyone, at every level, to understand at least the basics of cybersecurity. Most importantly, the general knowledge of it and how to mitigate daily risk factors. On a higher level, your entire organization must be protected, and all team members must work together towards a united goal of a well-protected enterprise organization.

After all, even a single data breach can devastate a company. The average total cost of a data breach in the US was estimated by IBM to exceed nine million dollars, and that's a bill most companies simply can't foot.

Developing a proper security framework is essential to ensure you have adequate protection to the parts of your business that are most essential to you and your clients' functioning.

Below are 3 important aspects of cybersecurity preparedness.

1. Risk Assessment from an Outside Perspective

Perspective really is everything in cybersecurity. You won't have the best protection to the threat landscape if you can't put yourself in the hacker's shoes. Have your IT team identify risks from a hacker's perspective. Developing a working strategy to prevent cyberattacks means looking for loopholes and weak spots that you wouldn't normally consider outright threats.

Remember, this isn't something your average IT person can do. If necessary, you'll want to hire a team of security experts to do the heavy lifting for you. Security experts live this world and have access to numerous environments to build their experience.

"Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015."

– Cybersecurity Ventures

A talented security expert will be able to identify openings or shortcomings in your current security and direct the best way to close any gaps. They can also assist with creating a plan for what happens should a breach occur.

By identifying each risk, making a plan and properly training those responsible, you strengthen your security posture.

This step helps to transform your security from reactive to proactive, reducing the overall risk you have while also strengthening your response to a breach.

2. Security Architecture

Once you've developed a security framework and completed an environmental assessment, you'll need to determine how your security architecture stacks up. Most organizations have perimeter security products. That includes things like intrusion prevention systems, email and web security products, endpoint protection services, VPN security clients, cloud security, and much more.

These are all foundational, but they're not enough to create a holistic security protocol.

Once you have the right solutions in place to meet the goals of your security framework, you'll need to focus your shift to tools that provide real-time insights into what's happening. After all, monitoring, analytics, and automation are all important parts of the overall security architecture.

All of this can become overwhelming, but partnering with security experts can help you develop a strong roadmap to keep you and your customers safe.

3. Educate Every Team

Member We briefly mentioned employee education earlier. But what does that actually entail?

Here are the top security issues employees should be kept abreast of:

Hacking

This type of cybercrime can cause huge financial damage to any company. In simple terms, hacking is when someone is able to access information without permission. This is done directly or remotely.

In most enterprise-level cases, hackers target unsecured website accounts and passwords to get access. Once they access your accounts, they can get their hands on your data. A hacker can then manipulate your data – either they'll destroy it, sell it, or hold it for ransom.

> **"According to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involved a human element."**
>
> **– Verizon**

Hacking is a broad term for a variety of different attacks. Nevertheless, the best practice to avoid hacking is to keep your passwords secure, your messages encrypted, and your common sense at an all-time high.

Identity Theft

Some hackers work on targeting specific people so that they can steal important data. If not protected, your team members may be unknowingly giving those hackers access.

In a practice known as “spoofing”, malicious actors disguise their communications to look similar to legitimate sources.

For example, spoofers may take the form of your boss sending you an email asking you to send personal information, such as a social security number or credit card details.

With this vital information, the scammer can further their ploy and use a victim’s identity to make purchases. But identify theft causes more than financial damage – there’s also emotional stress to consider, too.

The solution is minimizing spoofing attacks is to have 24/7 network monitoring and an active email filter to block these fictitious emails.

Still, the absolute best course of action is to train employees to recognize these false emails, usually denoted by their odd tone or incorrect spelling.

Malware

Malware is software that exists explicitly to harm or steal your information. In short, they’re computer programs developed for the sole purpose of corrupting and damaging other computer systems.

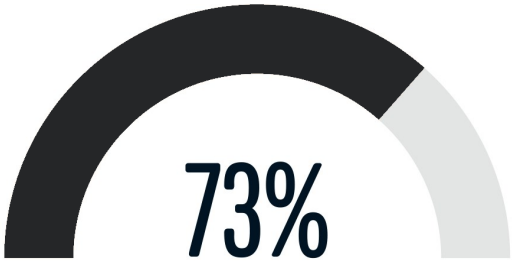
Malware is tricky to spot, as it often comes as an add-on to legitimate programs. But what’s worse than one infected computer? **Multiple infected computers**.

Malware can spread throughout the network and become a nuisance to deal with. To fight it, you’ll need to use robust antivirus programs and training that helps people understand how to avoid risky websites and fishy links.

The Evolving Threat

Landscape Of course, with more advanced technology come more sophisticated cyberattacks. We're now seeing the possibility of AI/Machine Learning (ML) software used by hackers.

In order to safeguard against these more sophisticated attacks, you must also use better technology to guard your critical assets.



"73% of firms fail cybersecurity readiness tests."

– Hiscox

As the cyberthreats evolve, take a proactive stance. We recommend having dedicated cybersecurity resources at your disposal. Look for trusted, experienced personnel you can count on to manage every aspect of your cybersecurity.

This way, you know for a fact that your organization is in good hands.

The Right Approach for the Right Outcome

Naturally, all of the above are huge challenges. With planning and a methodical approach to address these challenges, you put yourself in a much better position for success. It's never too late to bolster your security measures, and there's no better time than today to get started.

We design, deliver and operate our security services and solutions with care. A few of our services include:

- Assessments and road mapping
- Vulnerability scans and penetration testing
- Solution design and implementation
- 24/7/365 Managed Services
- Real people - local - ready to help!

With our team of highly certified professionals, you'll have all the support you need at all hours of the day.

Call us today to find out how you can be secure in every aspect of your organization.

Contact Us

https://datastrive.com

7738633868

6351 W Montrose Ave. Suite 204
Chicago, Illinois 60634