CYBER SECURITY AND DATA PROTECTION

PRIORITIZE YOUR CYBERSECURITY

Since 1996
Prescient Solutions

Table of Contents

Cyber Security and Data Protection

Cybercrime has grown significantly over the past few years, leaving both large and small organizations at risk. In addition to jeopardizing an organization's credibility, cyberattacks can damage their finances and productivity.

To protect your organization from data breaches, strong data protection and cybersecurity strategies are imperative. A business's ability to fight cybercrime will also depend upon its ability to recognize signs of a cyberattack and its readiness to respond.

What is Cybersecurity?

Cybersecurity is the practice of defending systems, networks, mobile devices, programs, and data from digital attacks. Cyberattacks often aim at intercepting, changing, or destroying private information; disrupting business operations; or extorting money through ransomware. Due to the growing number of devices and the increasing sophistication of attackers, implementing effective cybersecurity measures is particularly challenging today.

What is Data Privacy?

Often referred to as information privacy, data privacy involves the proper handling of data regarding consent, sensitivity, notice, and legal requirements. In its simplest form, data privacy refers to a consumer's understanding of their rights concerning how their personal information is collected, used, stored, and shared. Consumers should be informed of how their personal information will be used, and they must give their consent in most cases before any information is collected.

Why You Need Both

The best way for organizations to prevent data breaches is to integrate their data protection and cybersecurity strategies. When you look at recent data breaches, you'll find that most of them began with access to personal information. While unauthorized access to data is often perceived as a simple security breach, it can significantly impact an organization's cybersecurity.

By protecting your data, businesses will significantly strengthen their cybersecurity posture. With a coordinated data protection and cyber-security strategy, you'll have complete control over all stages of your data lifecycle. Additionally, you'll find it easier to comply with all regulations.

Conversely, cyber threats compromise your data's security. Hackers often target organizations' networks, systems, and programs to steal users' data. Many companies possess large amounts of data, making them attractive targets for cybercriminals. Therefore, increasing your cybersecurity strategies will help you protect your data.

Integrating data protection and cyber-security can also accelerate your organization's digital transformation. Through integration, data compliance and classification initiatives across the organization will be coordinated and aligned. Furthermore, it allows you to develop a uniform approach to cybersecurity and data privacy, which is critical to addressing emerging threats.

Repercussions of a Cyber Attack

Cybercrime can have several repercussions that can affect both individuals and businesses. Depending on the timing and duration of an attack, the impact of a breach may vary among organizations.

When assessing your security posture, however, you should consider the following impacts:

Digital

Cyberattacks can have devastating effects on the digital landscape that is targeted. It may require a complete redesign of your website. You may need to change your security procedures or create an entirely new social media account.

Financial

In the event of a security breach, cybercriminals may use unauthorized information to steal your assets. Your situation could worsen if you're unable to recover the money quickly. Businesses will also incur costs associated with repairing affected systems, networks, and devices.

Legal Consequences

Data protection and privacy laws require you to safeguard any data you hold about your customers or staff. The failure to deploy appropriate security measures may lead to fines and regulatory sanctions, regardless if your data is accidentally or deliberately compromised.

Reputational Damage

For companies that store personal information concerning others, a breach can have a devastating effect on how they are viewed. Even if you're well-known in your industry, a public leak might discourage people from doing business with you in the future.

Common Warning Signs of a Cybersecurity Attack

Having a secure network is like having a roof over your head – it keeps your business safe. Therefore, it's critical that you address a leak in your roof as soon as possible. Unfortunately, many people are unaware when they are being attacked until it's too late and their information has already been compromised.

To ensure that your network is protected from cyberattacks, here are five things to look out for:

An Unusually Slow Network

Cyberattacks or malware infections can result in spikes of network traffic that slow down the internet. A great way to identify unauthorized software is by checking the traffic logs of your device and the entire network. These steps will also help determine whether the software is consuming your bandwidth and what types of data are being transferred. When network speeds are significantly slower than normal, employers should notify the IT department immediately.

Files with Unapproved Changes

To avoid detection, hackers often change files once they gain access to your network. These changes can occur in a matter of seconds. Therefore, if your IT department fails to detect the change within a few minutes, it may go undetected for a while. Cyber security consultants can show you how to detect a file change before you are caught off guard.

Suspicious Computer Behavior

Your computer could be compromised if you notice suspicious or strange behavior. This could include finding extensions and toolkits you didn't install on your system. Your cursor control may scroll on its own without you moving the mouse. You may also observe frequent antivirus notifications when unnecessary. While system glitches may cause these behaviors, they could indicate a security breach if they occur frequently.

Login Issues

If you are having trouble logging into your account despite having the correct login information, you may be experiencing a cyberattack. Your login details may stop working for two reasons. The hacker may have locked you out after multiple attempts to access your account. You could also be locked out if your login details have been hacked and changed.

Data Loss

Missing data on your mobile device or online account may also indicate that your device or account has been hacked. Unfortunately, there's little you can do when this happens. Therefore, security measures and data loss prevention strategies must be strengthened before data theft occurs.

What to Do if You are Attacked

Despite your best efforts, hackers may still succeed in getting what they want. While these situations are uncommon, they do happen. In the event of a cyberattack, take these four steps immediately:

Contain

While it may be tempting to delete everything the hacker has accessed, it’s best to identify what has been compromised and quarantine it from your other devices. To ensure the rest of your devices and network remain safe after discovering a breach, follow these steps:

- Turn off remote access
- Ensure that all pending updates have been installed
- Ensure proper firewall settings
- Change your company's passwords immediately
- Disconnect devices associated with the breach from the internet

Analyze

As soon as the issue has been contained, you need to figure out how it happened. Analyze the affected servers, and determine whether anyone has access to them and which networks were active at the time of the breach. You should also determine how much of an impact it has had on your staff, clients, and customers. Find out if their data has been compromised and if there is a risk of financial loss.

Manage

Now is the time for transparency. First, let everyone affected know what happened and what data may have been compromised. Then, be available to speak with anyone affected. If necessary, establish a dedicated hotline for people to call. In the event of a security breach, being honest and transparent is crucial for preserving good working relationships.

Report

Finally, it's important to report cybercrime. Online crime victims are encouraged to file complaints at www.ic3.gov with the Internet Crime Complaint Center (IC3). The IC3 consists of the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Protecting Your Company from a Cybersecurity Attack

Mitigating cyber threats requires more than an antivirus upgrade; it requires ongoing attention. The good news is that protecting your systems doesn't have to be complicated. Here's how to get started.

Secure Your Databases and Networks

While databases can be a great way for companies to keep data and documents in one place, this doesn't mean they should store all information. Be selective in deciding what information is to be stored in company databases. Make sure your Wi-Fi network is hidden and password protected. In addition, setting up firewalls and encrypting data will help reduce the risk of cyber criminals gaining access to your networks.

Data backups should occur once a day or once a week, depending on the activity level within your organization. Having a backup of your company's data will increase your company's likelihood of surviving a cyberattack without losing all of its data.

Educate Your Staff

Discuss with your employees the importance of securing and protecting the information of their colleagues and customers. Establish policies that define acceptable and unacceptable practices. By limiting the number of users with administrative access in the company, fewer programs can be downloaded, reducing the risk of viruses and malware being installed.

Develop Security Policies and Procedures

Develop policies and practices to prevent cyberattacks and resolve issues if they arise. If an employee violates the policies, outline how it will be handled and what the consequences are. Prevent unauthorized access to company computers and handheld devices by properly controlling physical access and disposing of them.

As laptops and cell phones are easily misplaced or stolen, they are typically ideal targets for cyber theft. Therefore, when disposing of devices, reset them to factory settings. Bypassing this step can result in cyber criminals gaining access to company information.

Learn to Distinguish Fake Antivirus Offers from Real Notifications

Malware is a malicious program that collects information by sneaking onto devices via the internet, social media, email, attachments, and downloads. To prevent this from occurring, ensure your employees know how to recognize fake antivirus warning messages and immediately alert IT if anything suspicious is observed.In addition, establish a policy for your company's response to an employee's computer becoming infected with a virus. Finally, keep your security software up-to-date to prevent malware from entering your system.

Prioritize Your Cybersecurity

The fallout for businesses that are victimized by cybercrime can be devastating to their finances and reputations. While every business is vulnerable, every business can take critical steps to ensure its online security.

For enterprise-level data protection solutions, consulting with an IT firm specializing in data security is recommended.

Since 1996
Prescient
Solutions

About Prescient Solutions

Prescient Solutions is a managed IT services company specializing in infrastructure, networking, cybersecurity, cloud-based solutions, and help desk support. We are a leading IT provider with over 20 years of experience serving small, mid-sized, global, and government organizations. Using a cloud-based model, we help organizations of all sizes optimize their daily operations and manage their IT assets affordably.

From IT strategy to development and ongoing maintenance, our IT experts provide a full suite of remote and on-site services tailored to your business's needs. With today's technological landscape changing rapidly, our team is well-versed in the best options for your organization and uses proven tactics to implement them. Additionally, our IT solutions integrate seamlessly into your daily operations, allowing you to focus more on running your business.

Contact Prescient Solutions

1834 Walden Office Square, Fifth Floor
Schaumburg, IL 60173
(888) 343-6040 | prescientsolutions.com