HOW TO PROTECT YOUR DATA

Every day in the news, we hear about data breaches. Are you concerned your sensitive business, customer and supplier data is not protected?

Want to learn more? We are here to help!

STEP-BY-STEP INSTRUCTIONS:

1. Data Owner – All data needs someone in your organization to determine how valuable the data is that you want to protect. In the cybersecurity business, we call that person a data owner.

   The data owner could be the inventor who created your secret sauce, your CEO who devised your unique business strategy, or the customers who depend on your services.

   Not all data needs protection. The data owner can be called upon to determine which data to protect, how sensitive it is, who can access it and use it and the severity/criticality of the data if it is lost or stolen.

   It's easy to say that your payroll is critical for paying your employees, but the age of your equipment and warranty schedule, may be less important, until you need to replace it or ask the manufacturer to repair it if it is not working properly. The data owner for your business can help you decide how "critical" various data elements are that you want to protect.

2. Device Management - Data protection can include protecting the data by preventing access to the device (via passwords or other authentication methods) even while it is stored on a laptop or memory device. Ensure that any critical data stored on removable device (memory stick, disk, hard drive, laptop, tape) is password protected. These devices and the data that resides on them can be easily stolen and compromised. If the device is password protected, it will be harder to gain access to the data stored.

3. Cyber Safe Business Practices – simple business practices can help protect your data. Your employees are often your best defense in protecting your data. They know the ins and outs of your business, when deliveries are made, who the suppliers are, who your critical customers are, profit and loss data and many more unique business facts. Don't let that information get leaked, stolen or posted on social media.

   Here is a set of cyber safe business practices that you can easily implement:

   - Advise employees to routinely save their work, sounds simple, but hours of work could be lost if they don't think to stop and save.
   - Never open email attachments by habit or click on links unless it is a secure site and you know where the email originated.
   - Never allow employees to use memory sticks or disks from someone outside the company, unless someone has scanned it first for viruses.

- Keep your business operations private and instruct your employees about what can and cannot be posted on social media. Adversaries can use facts posted on public sites to conduct social engineering scams to trick your employees and compromise your operations.
- Advise your employees to keep their passwords safe and secure and use our guide on how to create secure passwords.

5. Hardware and Software – Data protection is also about protecting the devices you use to store, manage and track your data. Here are some simple tips to prevent data loss.

    - Hardware and software inventory life cycle status – do you know if your equipment is still supported by the manufacturer? Have you downloaded the latest updates? Does the vendor still support the applications you are using for your business? It is important to know where you stand in your inventory life cycle and whether it might be time to update your hardware and software. This is one of most overlooked cyber safe practices that criminals often use to gain access to your data.
    - Conduct regular maintenance and run virus scans, learn how to run a utility system that can diagnose your system for problems. These utilities can prevent little problems from becoming big problems, and will keep you in business.

6. Backups – Before you make changes to critical data, always make a duplicate. Even if you just made a backup yesterday, make another and label it. If you or your employees create a backup on a removable drive, have the drive or memory device password protected.

7. Off-site Storage – Something you probably never thought of, but what happens if there is a fire at your facility and your only backup was on-site and was lost in the fire? Keep a copy of your critical data offsite. If you use a managed service provider to store your data and applications, ensure that they provide you the ability to recover your data if it is compromised at their site. Know what is in the fine print before you sign the agreement. If they don't provide a guarantee - find another provider. Another option - one service provider may not be enough - you might need another provider in another region of the country to ensure your data is backed up – based upon your needs for recovery.

8. Encryption – Encryption is important to protect data during transit or at rest. Not all data needs encryption, in fact some important transmissions between your devices and the Internet wouldn't work if it were encrypted. Your wireless devices are constantly sending signals (transmissions) to your Internet service provider, telling it is ready to receive a signal or command. If everything was encrypted we wouldn't be able to enjoy many of the conveniences we do today at the speed we demand and expect. Learn how to encrypt your documents before you hit send. There are several very good low cost programs to encrypt easily.

9. Recovery Testing. Ok, you've made it this far, you believe everything is safe, you have a back up copy of your data at an offsite location and then poof – something happens and you need to recover your systems and data. But - you never tested your recovery procedures. Not a good place to be in!

    We recommend you develop a restoration plan and test the plan monthly. The restoration plan should have a number of features, such as back up schedule, restoration procedures (such as which systems to bring up first), how to conduct testing and how to copy your restored data back to your primary site operations.

"An ounce of prevention is worth more than a pound of cure."

COMMENTS/SUGGESTIONS/FEEDBACK ARE ALWAYS WELCOME AT WEB@THENCSS.ORG