

Data Security & Disaster Recovery

Planning Ahead is Critical to Reducing the Impact of Potential EDI Data Loss

EDI Resources Presented by 1 EDI Source

Volume 2, Issue 2

Data security and disaster recovery are critical to protecting EDI systems and keeping a business running. Become aware of data security issues and plan carefully for both daily security measures and the processes necessary to recover from a disaster.

EDI systems are crucial for managing essential communications between trading partners, transferring necessary data and assuring that vital documents, such as purchase orders and invoices, are processed correctly. If a company's EDI capabilities are lost, even for a short while, it can create a serious impact on the bottom line of the business. However, managers often fail to consider important safety nets for their EDI data, such as backups, redundancy and physical security measures.

Working to protect EDI systems and data means planning ahead and creating a system that works for your business. Following industry standard best practices, cataloging needs in the event of a disaster, and performing regular backups and recovery tests, are just a few of the ways managers may move toward improved security for EDI.

Impact of Data Loss

EDI systems were designed to manage the massive amounts of data that many companies need in order to properly operate and communicate with their trading partners. The digital world of modern EDI replaces the reams of paper previously needed to store physical records – and the space needed to store them.

That means, however, that EDI data is the only link between trading partners. Without proper security that link can easily be broken, resulting in the potential for lost orders, missed invoices, improper shipping and serious accounting issues – all of which may have an immediate impact on the financial status of a business.

Careful security in this world is all the more important because of the volume of data used, and the frequency with

KEY DECISION



What do I need, at minimum, to protect my company's in-house EDI system?

- A disaster recovery plan
- Carefully tested backups performed at frequent intervals
- Secured communications between trading partners via AS2 or secure FTP
- A secure off-site location for your backup files
- A physically secured data center that requires password entry by selected individuals

which it passes between trading partners on a network. In this environment, every minute lost to an outage can have an effect. Things as simple as a down internet connection or an office power loss may become serious events if not resolved quickly enough to get the EDI system functioning for its next tasks.

Moreover, the data contained in an EDI system represents not only information specific to the company using the system, but also potentially sensitive data from its trading

KEY DECISION



What sort of events should my disaster recovery planning cover?

- Hardware failure
- Power loss
- Fire
- Flood
- Building environmental system failure
- Lost internet connections
- Software glitches
- Loss of key employee

partners, and private information about individuals, as well. Securing these systems is an important step toward protecting necessary information for all of those involved.

Expect the Unexpected

Remember, strong security is not just about the events you can anticipate. Rather, it is about preparing even for the sudden and unforeseen. Data can be lost through intentional theft, system failures of various types and natural disasters that cannot be controlled but for which you can prepare.

One of the major mistakes companies involved in EDI make is failing to recognize the number of things that can happen to their systems. Hardware failure is a reality that makes itself known at the worst possible moment. Lost internet connections can mean lost time and lost data as well. And system failures may occur for no obvious reason, or because of simple human error, such as failing to properly test systems connected to the EDI system during systems upgrades or other infrastructure changes.

Disaster recovery success rests on being ready for the potential of total system failure due to fire, flood, or even problems with a building's environmental system. Any of these – and many other – events may render hardware useless and if redundant systems are not available serious data loss can occur.

Whether you operate your own EDI systems or out-source with an EDI service provider, protecting your EDI data begins with awareness and planning. Make security a part of your daily routine and think constantly about ways to improve it. Work with software and hardware providers to implement industry standard best practices and look carefully for the providers you can trust.

Protecting In-House Systems

Operating EDI in-house means a commitment to security that is both thorough and tested. Take the time to think carefully about the physical assets used in EDI, how the data is transferred to trading partners, who has access to that data and what would happen if the data center was permanently damaged. Review processes for security planning, implementation and disaster recovery.

The first word in in-house security is backup – and it is also the first word that many companies forget in the rush of daily activity. Set up automatic backups to run daily at the very least, more often depending on the volume of EDI data processed. Look carefully at what data must be included. EDI backups need to contain everything so that if the main data

KEY DECISION

What security steps should I expect from my EDI provider?

- An off-site replicated data center at a secure location
- Physical facility security including password entry and steps such as fire suppression
- Carefully secured communications protocols where appropriate
- Individually secured data
- Redundant power and internet systems
- Dedicated consultant that has a working knowledge of your EDI environment

center machine burns to the ground, the company can be quickly operating again somewhere else.

Think about backups in terms of each step in the EDI process. A backup will be needed for EDI data, maps, trading partner set-up information and custom configurations – just to name a few essential components. And do not forget to have a backup of those internal systems that are connected to the EDI system as well.

Backups should never be taken for granted. Just because they exist is no reason to assume they will work properly when they are needed. Make sure to test your backup system regularly and, most importantly, backup files should not be kept right next to the main system. Find a secure off-site location and keep them there.

EDI systems function not only through data, but through the transfer of that data between various trading partners. These communications should be secured by using a data transfer method that reduces the chances of outside parties

accessing the data in transit. Some options include Applicability Statement 2 (AS2) or secured FTP transactions.

The opportunity for your data to be used by others can also be lessened by considering the physical security of your EDI assets in-house. For example, restrict data center entry to those individuals who must use it, and require a password.

Appropriate in-house security is largely dependent upon your type of facility, the sort of data with which you are working and its amount. Work with your software and hardware providers to understand the best practices they suggest and how those can be implemented in your environment.

Carefully established security processes should be shared with appropriate staff members. Have a written procedure available to instruct personnel on how to utilize the backups and emergency contact information for technical support, including backup technical support in case a particular individual is unavailable. Work with your colleagues to create an environment with the best chance to get your EDI system up and running quickly in the event of a failure.

Security with EDI Service Providers

When you choose to outsource your EDI needs, you entrust an outside company with the operation of, and security for, some of your most important business data. It is absolutely essential, therefore, that you take the time to find a company you can trust with this vital function.

Look for an EDI service provider in the same way you would search for any strong business partner. Ask about the type of hardware they will use to house and process your data. You should expect this to include tier 1 hardware names that you easily recognize. Pose questions about the internet bandwidth available, certified technicians on staff and the specific security processes in place to protect your data from theft or recover it from disaster.

Your data must be back online and available as quickly as possible in the event of a disaster. EDI service vendors should

operate frequent backups that are carefully tested and those backups should be housed at a secure off-site facility. Moreover, you should expect your provider to operate redundant servers so that data is replicated in multiple locations frequently, including an off-site location. This way, if the worst should happen, your data will be back swiftly and data loss will be minimized.

An outsource provider has a particularly high threshold for security expectations because of the amount of data being moved at any one time. Look for systems that are individually secured and hosted in a dedicated environment so that the data files of various clients do not touch one another. When each client is part of their own workgroup and security is set specifically for them on the server, it reduces the chance of all clients being exposed if a security breach of some kind occurs.

Not only should your EDI provider demonstrate the ability to secure communications between their facility and your trading partners, they must also consider the importance of securing appropriate communications between their clients and themselves. This attention to detail regarding security matters is crucial.

Further, EDI service providers should constantly monitor their communications software, EDI systems, backups and other connected systems to ensure that everything is always functioning properly. Carefully designed and implemented monitoring tools and procedures should ensure that the EDI service provider discovers any problems or issues – *before* their client or trading partner is impacted by them. When searching for an appropriate EDI service provider, ask questions about what systems are monitored, how often the monitoring occurs and review the provider's escalation procedure so that you know the steps they take when problems arise.

Of course, the best way to secure data is to attempt to avert disaster in the first place. The facilities offered by EDI service providers offer physical security measures to lessen the chances that the system will go down. Steps may include an advanced fire suppression system, 24-hour secured entry to the facility, redundant power via batteries and generators and even redundant internet connections. ♦

1 EDI Source Solutions

1 EDI Source is your source for everything EDI, including EDI Software, AS2 Software, ASN Software, Web-based EDI Services, EDI Consulting and EDI Outsourcing Services. For nearly 20 years, 1 EDI Source has been committed to providing reliable and affordable EDI solutions and expert EDI advice to companies of all sizes, and continues to maintain and develop strong business relationships in the retail, consumer packaged goods, manufacturing, education, financial services, transportation, health-care and telecommunications industries.

Our in-house experts design flexible, customizable solutions that work specifically for your business. You'll receive one-on-one attention to your needs, assistance with critical set-up and maintenance of your EDI system and an entire team of professionals available anytime.

Visit www.1EDISource.com to learn about our full line of products, or call an expert for more information at 877-334-9650.

1 EDI InSource™

Advanced software solutions including EDI software, ASN software and AS2 software

1 EDI OutSource™

Complete, expert outsourced EDI solutions

1 EDI WebSource™

Easy-to-use, affordable web-based EDI services

1 EDI ReSource™

Expert EDI training and consulting services