There’s just one thing as sickening to a business owner as experiencing a loss of data, which is knowing that loss was completely avoidable had there been a legitimate data backup and disaster recovery plan in place.

Proper data protection is crucial for any business, yet many businesses—especially small ones—are vulnerable to catastrophic data loss and lack a backup and recovery plan. Even worse, many businesses are unaware of their own susceptibility to data loss.

**What Does Data Loss Mean For Your Business?**

Losing critical data for your business is like losing a critical piece of yourself— you would never feel whole. That’s what it’s like for your business after suffering some sort of data loss.

It doesn’t matter where or how data is stored—data storage systems fail, and they fail with a spectacular frequency.

Your business could lose all of the data you have about your customers, your product and service records, proprietary business documents, financial records, employee records, purchase order and payment information—there’s just no shortage of the types of data that could be lost.

Essentially you are losing a documented history of your business and it doesn’t just impact you, or your business. It impacts every single person or business you’ve ever done
business with and leaves you liable for all of that personal information that was lost.

Knowing what all you are likely to lose, you now know it could be literally impossible to conduct business the way you were after suffering a severe data loss of this kind.

**What Can Cause Data Loss?**

**Human Error** – accidental or unknowingly deletion of data, modification, or overwriting files

**File Corruption** – software error, viruses and malware infections

**Hardware** – drive failure, cpu failure, cooling system failure

**Site-Related** – natural disasters such as flooding, earthquakes, lighting strikes, or fires and even theft

According to a report on data loss, the rates in which these events occur are:

“According to a business audit conducted by DTI/PricewaterhouseCoopers, 70% of small businesses that suffer a significant data loss are out of business within a year of that event.”
The Importance of a Data Backup and Disaster Recovery Plan

- Hardware Failure (42%)
- Human Error (31%)
- Software file corruption (13%)
- Virus infection (7%)
- Theft, predominantly laptop theft (5%)
- Hardware damage/loss (3%)

**What Happens to Businesses After Data is Lost?**

According to a business audit conducted by DTI/PricewaterhouseCoopers, 70% of small businesses that suffer a significant data loss are out of business within a year of that event. Even if, and it’s a big if, you don’t suffer a total loss and are capable of recovering something, the downtime your business would experience could be equally devastating. Let’s say your business earns $5 million in annual revenue and your entire system goes down due to some disaster – whether someone downloaded something onto the network they shouldn’t have (which happens far more often than you’d think), your physical server crashes, or something else happens at your physical location – you are still missing out on critical productivity.

Think of your business as an employee, and with 2,080 total work hours in any given year, your business earns $2,403.85 per hour. Even if you are only down for five hours, which is a very conservative estimate without a backup and recovery plan in place, you’ve just lost more than $12,000. If you are out of commission for 10 hours, which is far likelier without a recovery
A Data Backup and Disaster Recovery Plan Should Not Be Overlooked

As the examples above have illustrated, your business suffers when you choose not to take precautions in protecting your data and having a proper plan in place to deal with disaster and data loss that accompanies it.

Having an actionable data backup and disaster recovery plan is more than just backing up your data every once in a while though. A proper plan, such as one that the backup and disaster recovery experts at i.t.NOW have experience crafting, must cover every contingency and must be regularly tested to make sure it is functioned as designed.