proActive tech group

The Data Loss Case Files

Major U.S. Companies Data Loss and the New Strategies We've Learned as a Result

www.ptg.co


6Gb SAS FRU
42D0833
146 GB
6Gb SAS FRU
42D0833
146 GB
MT: 7870 S/N: 06BD402
Product ID: 7870B4A

Table of Contents

Introduction

Data loss. No two words strike fear into the heart of businesses large and small, quite like those. And with good reason. Data loss and the resulting downtime can wreak havoc on your business finances and operations. Cyberthreats are on the rise. Negligence alone has the power to disrupt and destroy.

A business owner who doesn't feel exposed isn't paying close enough attention. Data is the lifeblood of today's economy. Unfortunately, that means it's also the lifeblood of the hacking world, too. Ransomware, general malware, incompetence, rogue employees … there are a ton of ways your company's data can be compromised, stolen, or completely wiped out.

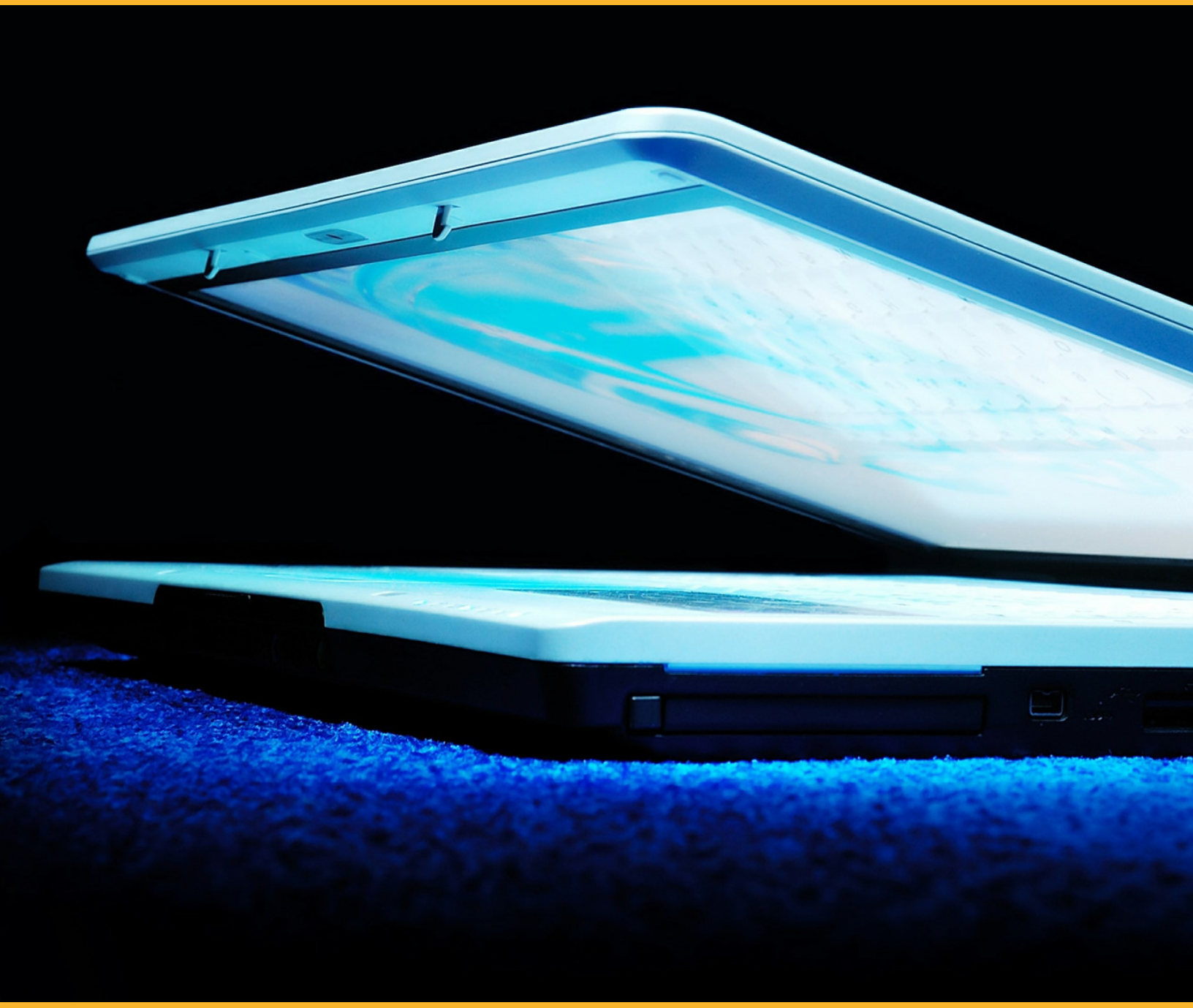
Here's the good news. There are also a lot of strategies to avoid or minimize the potential for business data loss.

In framing the problem, it can be particularly helpful to look at lessons to be learned from other company's past mistakes. With the right solutions and the right recovery plan, you can effectively protect your business from a large majority of data loss incidents.

In the process, you can stop inconvenient from becoming catastrophic and unavoidable from becoming unrecoverable.

Let's take a look at 5 data loss stories from companies of all sizes that span the breadth of potential threats. While we're at it, we'll explore what you can learn from each incident to avoid becoming yet another data breach statistic.

26 Million US Veterans' Data Lost to BYOD Theft



The government is hardly immune to data loss. And while there are numerous stories about government data loss, one stood out as a demonstration of just how vulnerable even the federal government can be.

In 2006, a laptop was stolen from a Department of Veteran Affairs (DVA) data analyst's home. The laptop contained a whopping 26.5 million US military veterans' social security numbers and birthdates, among other sensitive information.

The DVA panicked and mounted a full-scale nationwide response. The laptop was ultimately recovered after offering a $50,000 reward for its return. And while it may seem like good news that the FBI determined no data had been copied or compromised, that doesn't tell the whole story. Not long after the event, a class-action lawsuit was initiated by the soldiers whose data had been put at risk.

The DVA ultimately settled this class-action suit for over $20 million. That's a ton of public cash to pay out for one stolen laptop. Especially given that there are solutions that could have avoided all the concerns.

The Lesson:

Can your business afford a multi-million dollar lawsuit? How about a multi-thousand dollar lawsuit? Whether SMB or enterprise-level, you probably want to hold on to all the money that you can.

This is why you have to be responsible almost to the point of paranoia about the vulnerabilities that bring your own device (BYOD), as well as allowing employees to take work devices home, adds. After all, you can be held legally responsible when sensitive data is compromised through negligence or theft.

Don't take it the wrong way. BYOD is a fantastic way to increase productivity, and it's here to stay. But it has to be tempered with proper security protocols to remain an effective and attractive approach.

Two of the easiest ways to shore up this vulnerability:

1.) Require any device used to store or access sensitive data to be password-protected. And don't sleep on proper password complexity, either.

2.) Take advantage of remote wipe apps and programs to empower your company to wipe sensitive data and access remotely in the event a device is lost or stolen.

Ma.Gnolia Lost All Its Data and Went From Hero to Zero Overnight

If you're like most businesses, one of your main goals is to remain in business for as long as possible. That's a no-brainer, which is why you should be deeply concerned with potential data loss and the effects it can have on your business life cycle.

The requisite horror story example is Ma.Gnolia. The social bookmarking company was once the talk of their industry. That is, until all critical servers went down, corrupting all their data in the process.

And check this out: They had a backup, too. The problem was that their backup server was onsite, rather than off-site. The corruption that rendered all their initial data unusable was pushed to the backup copy as well.

The result of this absolute fiasco was that the company lost every single shred of their users' saved data, and closed up shop a year later after a failed rebranding attempt did nothing to salvage their reputation. You can imagine consumers weren't happy when the company they trusted specifically to save their bookmarked data for them lost all the bookmarks.

The Lesson:

How valuable is your brand? How resilient would your company be to 100% data loss? Those are rhetorical questions for most businesses. Your brand IS your company. Your data is the lifeblood of that company. Very few businesses could survive without either.

Data loss destroys reputations. Customers can and usually do have other options for your service. Ma.Gnolia's certainly did. You NEVER want to give them a reason to use them. And even if you could theoretically retain your customers after catastrophic data loss, would it matter if you lost the functional data you used to service them? Probably not.

Two critical ways to shore up this vulnerability:

1.) Develop and implement a disaster recovery plan. Practice it. Know it. Update it. Do not wait until the unthinkable happens to try and salvage your company's reputation.

2.) MAKE SURE you have a data backup service that is reliable and undergoes periodic testing. That service should have multiple redundancies, and these should INCLUDE off-site backups from the main data center where your data is backed up and stored. Follow the 3-2-1 rule, which includes one off-site backup copy.

Equifax Lost 148 Million Users' Credit Report Data (And Its Credibility, Too)

Can you think of any company with access to more sensitive data than a credit bureau? Probably not, which is what made Equifax's 2017 web data loss event so astounding. The breach affected more than 148 million users, whose sensitive data – including social security numbers, birthdates, and addresses – was compromised.

Worse, 209,000 customers had their credit card information compromised. In the wake of the scandal, Equifax created a special website to deal with customer communication regarding the breach and contacted each customer by US mail. The company also had to voluntarily begin providing its credit monitoring services for free to the affected customers.

The cost of these reputation management and recovery procedures? $4 billion so far. And that's just the cost to their stock market value. One can only imagine that the long-term costs, which remain to be seen, will be far worse.

So how was Equifax hacked? Was it some astoundingly sophisticated hacking job that couldn't have been avoided? Afraid not. The hackers took advantage of a security flaw in an open-source software called Apache Struts – a known flaw the company had neglected to address for months.

The Lesson:

Update your software. No, really. Do it now. Do it often. Don't take it lightly. Often software updates contain patches to known security gaps and flaws. Guess who else either knows or will know about the same flaws in short order? Hackers.

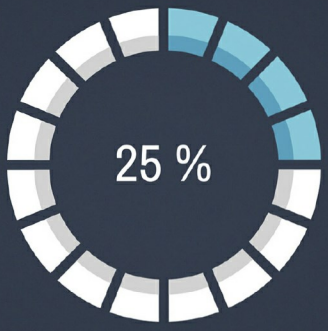
This same lesson was learned recently with the WannaCry ransomware incident. In that case, the only users affected were those who had not bothered to perform the latest Windows update.

Here are two pieces of cybersecurity "hygiene" to practice:

1.) Either make sure your IT department has dedicated employees constantly making sure all your software and programs are up to date, or …

2.) Partner with a qualified Managed Services Provider who can either oversee your network, provide cloud services, or both. The right MSP will have multiple solutions that can help protect your network and raise productivity in the process.

Updating



CANCEL

click here for more information

Anthem Suffered the Largest Breach of Healthcare Information in History

In February 2014, Anthem Healthcare got breached for a shocking 78.8 Million consumer records. In case it needs saying, that's a lot. The cause of such a massive breach? A single user within the network falling victim to a phishing email. Let that sink in. A negligent mistake from an individual user in their network caused a leak of 78.8 million records.

The breach likely cost the company something in the neighborhood of $100 million. The consequences for those whose data was compromised could well reach into the trillions before it is all said and done.

The Lesson:

We've talked about the liability aspects of data loss and breach. No need to rehash them here. But there's a huge lesson to be learned about the potential damage of insider threats to your network. All it takes is one irresponsible, uneducated or negligent user within your network clicking on the wrong email to bring your company to its knees.

Here are two simple things you can do to help avoid such catastrophe:

1.) Provide extensive and ongoing training to your employees on how to spot phishing emails and best practices to avoid contracting malware and ransomware in general.

2.) Implement the principle of least privilege for employee login credentials. By limiting the amount of data, application and systems their logins can access, you can also limit the extent that malware and ransomware can infect your system.

Toy Story 2 Almost Lost a Year of Animation Data After a Faulty Delete Command

We love Woody, Buzz, and the gang as much as anyone, which is why this story is shocking. The enormously successful *Toy Story* franchise almost took a death blow when someone working in Pixar's network accidentally ran a server command that rapidly began deleting animation files.

According to eyewitness accounts, animators had to watch as the iconic characters began disappearing one piece at a time. Picture watching Woody's hat disappear, then his vest. Then his boots and shirt.

In less than 20 seconds, an entire year's worth of animation data vanished. But that's not the tragic part of this story.

When Pixar's administrators went to restore backups of the lost data, they made a horrifying discovery. The backups had failed during the last month, unbeknownst to anyone. Without the now-lost files, they were facing the prospect of reanimating the entire film.

Fortunately, this story has an incredibly lucky ending. That's because the film's technical director, Galyn Susman, had been working from home after the birth of her child. Against company policies, she had stored the data on her personal hard drive. If not for this, the entire movie would have been lost, and the hit movie we know today could have been entirely different in execution and animation.

The Lesson:

Check your backups. No, really, check them. You need a tool or service to check them often. Many companies have been shocked after a downtime or data loss incident to discover that their backups have partially or completely failed.

Backups won't do you any good if they stop working or don't update frequently enough. In some ways, this can be as harmful as not having them at all, because of the false sense of confidence it provides.

Here are two simple things you can do to avoid becoming another data loss warning story:

1.) Stop storing data on hard drives alone. They fail at incredible rates. All data should be backed up either on company servers or, preferably, in the cloud.

2.) Make sure your backup and disaster recovery plan includes periodic testing and checks to ensure your data is being backed up properly. Also, makes sure the backup partner you choose has the right levels of redundancy in place. Failure to see this particular step through could result in major, business-ending consequences.

Statistics Don't Lie: Data Loss Can Crater Your Business

Now that we've covered a few data loss disaster stories, let's take a look at some of the more powerful statistics and coming threats. The numbers tell a powerful story of financial and operational risk for your business.

"Number of records breached in 2016: 1,378,509,261."

Source: Gemalto Breach Level Index

The Takeaway: With more than a billion records breached in 2016, and 2017 numbers predicted to have risen dramatically, it's clear that cybercrime continues to be on the rise. Which means that businesses' approach to dealing with cybercrime will need to continue to evolve.

"60% of SMBs who lose their data close within six months."

Source: Clutch

The Takeaway: What seems clear is that the smaller the business, the more catastrophic the data loss and downtime can be. Simply put, most SMBs ultimately cannot recover from a serious data loss incident.

“Nearly half of IT providers say phishing emails are behind ransomware attacks.”

Source: Solutions Review

The Takeaway: To be more exact, the number is 48%. But 36% of those providers report that a lack of proper cybersecurity training for employees was to blame. It seems clear that proper training can have a significant impact on your potential for falling victim to a ransomware attack.

“66% of data protection leaders admit that employees are the weakest link in an enterprise’s security posture, and 55% of organizations have had a security incident or data breach due to a malicious or negligent employee.”

Source: Ponemon Institute

The Takeaway: Your employees matter. Train them well, and make sure you hire employees you can trust. When employees are released for any reason, it is critical to restrict their access immediately to prevent data loss or theft due to malicious intention

“One laptop is stolen every 53 seconds, and over 70 million cell phones are lost each year.”

Source: ChannelPro

The Takeaway: In the world of BYOD, that’s a lot of rogue devices. Considering that only 7% of the lost cell phones in particular are ever recovered, it’s a recipe for crazy amounts of data breach and loss. If your company doesn’t already have an extensive BYOD policy that includes requiring passcodes on every device that accesses the network, create one now.

Recap: 10 Strategies for Data Protection

Data loss is expensive and more common than many people think. SMBs in particular often seem to operate with the “it won’t happen to me” mentality. But data loss, whether through a breach or a lack of backup, is common for companies of all sizes.

Let’s recap some of the strategies we’ve discussed to clarify and organize them into a single stream of useful data you can put to work in your business. We’ve distilled the lessons down to 10 strategies that are crucial to protecting yourself from data loss for your convenience.

Failure to secure and protect your data from loss can lead to legal liability and general financial loss.

Strategies to protect your business:

1.) Require all network-accessible devices to be password-protected. Focus on proper password complexity.

2.) Employ the use of remote wipe apps and programs to protect data on lost devices.

Your brand and your reputation are one – 100% data loss can destroy them both.

Strategies to protect your business:

3.) Develop and implement a disaster recovery plan.

4.) Employ a reliable data backup service that has multiple layers of redundancy (including off-site backups) and undergo periodic testing. Follow the 3-2-1 rule, which includes one off-site backup copy.

Outdated or unpatched software has vulnerabilities that put you at risk for ransomware and malware attacks.

Strategies to protect your business:

5.) Either make sure your IT department has dedicated employees constantly making sure all your software and programs are up to date, or partner with a qualified Managed Services Provider who can oversee your network, provide cloud services, or both.

One negligent or malicious employee can cause massive data loss and security breaches.

Strategies to protect your business:

6.) Provide extensive and ongoing training to your employees on how to spot phishing emails and best practices to avoid contracting malware and ransomware in general.

7.) Implement the principle of least privilege for all employee login credentials.

Many companies' data backup systems fail without their knowledge, leading to lost data in critical moments where restoration is needed.

Strategies to protect your business:

8.) Stop storing data on hard drives alone. They fail at incredible rates. All data should be backed up either on company servers or, preferably, in the cloud.

9.) Make sure your backup and disaster recovery plan includes periodic testing and checks to ensure your data is being backed up properly

10.) Enlist the help of a qualified backup specialist to oversee your backup process, schedules and testing to prevent corruption or failure.

Conclusion

Data loss is a frightening proposition. But it doesn't have to be. By taking the time to line up your business strategies and create proper security levels, as well as backup redundancy, you can protect yourself from the vast majority of data loss woes.

No company is completely insulated from harmful threats like malware or ransomware. However, with a proper focus and the right tools and partners, you can take a safe approach to your business data that protects your growth, reputation, and finances for the long haul.

By the way, data protection is what we do. We have years of experience assisting companies with everything from data loss to network security to employee training. We have the knowledge, expertise, and resources required to shore up vulnerabilities, proactively protect your data and educate your team on best practices to avoid network breaches.

Contact us if you would like more information on the subject, we're happy to take the time to see how we can assist your business.

516-876-8200

14 Plaza Road
Greenvale , New York 11548

www.ptg.co