HOW MUCH DOES DATA LOSS COST?

You're busy running a business or starting up a new venture. Data loss is just one more thing to mind, and it's one you'd rather not think about.

Yet data loss has a significant impact on businesses, especially small businesses. You've heard the warnings and read about the threats, but have you thought about the full financial implications of data loss?

This eBook explores what we know about the costs of data loss.

Businesses of different sizes and industries will always share one commonality: cybersecurity threats. Verizon's extensive Data Breach Incident Report (DBIR) in 2022 noted that "contrary to what many may think, very small organizations are just as enticing to criminals as large ones and, in certain ways, maybe even more so." Worse still? A security incident can lead to small businesses shuttering for good.

The exact dollar value of data loss can vary widely. The cost depends on the nature of the data, the business size and industry, and the extent of the data loss. Yet compromise of sensitive or confidential information is costly in many ways.

Before examining data loss costs, we'll first outline some causes of security incidents. Don't worry, this discussion isn't all depressing. We close with best practices to prevent data loss that you can apply at your business.

CAUSES OF SECURITY INCIDENTS

Studies of data breaches and their financial impact consistently highlight large costs. Large-scale breaches can reach into the millions, even billions. But what causes these security incidents? In its 15th annual DBIR, Verizon cautioned against the following actions:

ERROR

Incorrect or inadvertent actions that cause cybersecurity vulnerabilities.

SOCIAL ENGINEERING

Deceiving, manipulating, or intimidating users into providing access credentials or funds.

HACKING

Unauthorized access of computer systems, networks, or devices to manipulate, disrupt, steal, or destroy.

MALWARE

Malicious software, script, or code that alters a device's state or function, done without the owner's knowledge and consent.

EMPLOYEE MISUSE

A trusted individual accesses business resources in unauthorized and unintended ways.

PHYSICAL

Accessing secure premises and taking possession by proximity or force.

ENVIROMENTAL

Natural events and environmental hazards can threaten data assets or infrastructure.

FLAG Computer Repair

OVERALL COSTS OF DATA LOSS

Estimating the dollar value of data loss is challenging, as there are a multitude of factors involved. It's also difficult to value intangibles such as damage to business reputation.

Still, researchers try to calculate the financial implications of data loss:

Globally, the average cost of a data breach was $4.35 million. That works out to approximately $164 per record, per IBM and the Ponemon Institute.

Verizon found loss or compromise of around 100 records cost businesses an average of $18,120 to $35,730.

Large-scale data loss (100+ million records) costs an average of $5 million to $15.6 million, per the DBIR.

HOW DO DATA BREACHES ADD UP SO FAST?

Data loss has several costs factors. After data loss or a breach, your business bottom line gets hit from many directions.

COST OF RECOVERY AND REMEDIATION

Data compromise often leads businesses to invest in recovery efforts. This can involve data restoration and forensic analysis. The more complex or large scale the incident, the greater the recovery costs. Plus, you may need to pay to enhance your security measures going forward.

One American school district lost access to its data and systems in a 2020 ransomware attack. Recovery efforts cost Baltimore County Public Schools in Maryland almost $10 million.

PRODUCTIVITY AND OPERATIONAL LOSSES

Data loss can significantly disrupt business operations. Addressing a breach can decrease productivity, make you miss deadlines, and lose revenue. Employees aren't happy either, which can be problematic during the "Great Resignation."

Lose any critical data permanently? Expect further delays and increased costs. You could need extensive efforts to recreate or recover that lost data. A leaked password disrupted fuel supplies across the southeastern United States. The 2020 ransomware cost alone was $5 million in cryptocurrency. The six-day Colonial Pipeline shutdown also increased gasoline prices and meant lost revenues.

FLAG Computer Repair

THREAT TO INTELLECTUAL PROPERTY & TRADE SECRETS

Losing your intellectual property or trade secrets could have severe consequences. Consider the damage if a competitor gains access to your secret sauce recipe. Losing your competitive advantage could cut your market share and reduce revenue.

In 2017, a ransomware attack cost global pharmaceutical giant Merck roughly $870 million. The attack crippled production facilities. Merck had to borrow 1.8 million doses of an HPV vaccine from an emergency supply. It took 18 months to replenish the stockpile.

REGULATORY AND LEGAL CONSEQUENCES

Loss of data can lead to legal proceedings and regulatory non-compliance. Your business could face regulatory fines or penalties and potential lawsuits.

The Cyberspace Administration of China fined Didi Global $1.19 billion (8.026 billion yuan). They charged the ride-hailing company with violating three national security laws.

LOST OF CUSTOMER TRUST AND LOYALTY

Data loss incidents often erode customer trust and loyalty. Customer churn will reduce revenue. At the same time, acquiring and retaining new customers could cost more after data losses.

A Sage employee gained unauthorized access to employee data and compromised customer data. The UK accounting firm's share prices fell by as much as 4.3 percent.

BEST PRACTICES TO PREVENT DATA LOSS

In 2017, Equifax saw the personal information of approximately 147 million people compromised. Legal fees, investigations, customer support, and cybersecurity improvements cost the credit reporting agency nearly $2 billion.

Your business may not suffer a data loss of that scale or financial impact, but you'll still want to take action to protect your data and secure your systems.

Here are 10 best practices to help prevent data loss:

1. Back up important data using both on-site and off-site backups.
2. Limit user access privileges to only what is necessary for their roles.
3. Enforce strong, unique passwords, and consider implementing two-factor authentication (2FA) for added security.
4. Keep software and systems patched and up to date.
5. Educate employees on cybersecurity awareness.
6. reputable antivirus and anti-malware software on all devices.
7. Watch and control incoming and outgoing network traffic.
8. Use secure Wi-Fi networks with strong encryption.
9. Encrypt sensitive data.
10. Regularly test and assess security measures.

THE TRUE VALUE OF CYBERSECURITY

Calculating the cost of a data loss is difficult. Save your math acumen for something more positive. Instead, work with a managed service provider to secure data and IT infrastructure.

Our experts can help develop business continuity solutions and backup your computing infrastructure.

Let us help protect you from the catastrophic costs of data loss.

FLAG Computer Repair

Phone: **07976151148**

Email: gary@flagcomputerrepair.co.uk

Web: www.flagcomputerrepair.co.uk

Facebook: facebook.com/flagcomputerrepair.co.uk