Data Breaches and Their Impact on Business

FILECLOUD
WWW.GETFILECLOUD.COM

Executive Summary

Data breaches are increasing in volume and velocity at an alarming rate. The International Data Cooperation estimates that a quarter of the global population will suffer from a data breach by 2020. To keep their valuable data safe, companies must prepare for the numerous threats to personally identifiable information.

Unfortunately, despite their best efforts, businesses often fail to contain the impact of a data breach. What happens then? Find out more about the impact of data breaches on modern businesses

> *"FileCloud enables data infrastructure modernization scenarios, thanks to its flexible cloud implementation, backup and disaster recovery support"*
>
> **Gartner magic quadrant report**

> *"FileCloud is deployable in a private cloud (FileCloud Server), a public cloud (FileCloud Online) and hybrid architectures. Organizations can choose to implement FileCloud on public cloud infrastructure, such as that of AWS and Microsoft Azure, or private data centers."*
>
> **Gartner magic quadrant report**

Immediate Impact

As soon as a cyber-attack is detected, your external vendor partners and tech team launch a plan of attack. This covers everything from damage control to fixing the vulnerability that enabled the breach in the first place to ensuring data restoration from external backups.

However, the truth is, each of these processes takes precious time away from your regular operations, while negatively affecting your overall manufacturing, customer service, staff productivity, and e-commerce in general. Also, your business might incur additional expenses if you hire external consultants to restore your data access and operations. On top of that, there are expansive regulatory issues that need to be taken care of, including regulatory filings and technical investigations regarding the breach and its impact on your consumers.

While it is possible to quantify these costs with little effort, some hidden expenses lurk behind the scenes when the data breach is extensive. Companies are used to invoices of thousands of hours billed by forensic analysts to piece together the actual nature of the data breach.

Research shows that almost a third of customers will discontinue their relationships with finance and healthcare organizations if they've experienced a data breach. Apart from that, victims will notice an increase in the cost associated with acquiring new customers.

Negative effects on chain-of-command

A lot of cyber-attacks are the work of outsiders who intend to steal sensitive proprietary data and PII. Malicious entities deploy their attacks usually through email, with nearly 30 percent containing some form of malware.

Most businesses have a hierarchical structure in place, which makes it easier for hackers to follow the chain-of-command. Thus, cybercriminals do not have to resort to brute force attacks to breach the secure networks of your business. Rather, they target employees and staff in phishing attacks, often installing the malware in their systems or impersonating executives

Long-Term business impact

Most organizations consider information security an IT issue instead of something that can put your entire business operations in jeopardy.

Monetary impact

Cost is the first thing that comes to mind when you consider the business impact of a data breach. If your attackers focus on your money, you might never get it back. Also, you are paying consultants and employees extra to work hard and resolve the issue as quickly as possible.

If the attack is large-scale, you might need to hire a lawyer to represent your company. But none of this takes into account the fine that you might have to pay to regulatory bodies. Data breaches often cost so much that small and medium businesses have no choice but to permanently shut their doors.

Business reputation

Even though it is more difficult to gauge, your organization’s reputation takes a hit after a data breach. Consumers find it difficult to trust brands already. So, there’s no going back if you accidentally leak their personally identifiable information. They will take their cash as well as their loyalties with them.

Collateral damage

The impact of a business data breach goes way beyond dollars. While a few consequences cannot be measured, they are still significantly impactful. Critical data may fall into the wrong hands, or get lost forever. Plus, trade secrets, sensitive employee data, or intellectual property being stolen or lost is detrimental to your company.

Your systems may be held ransom, leading to downtime. Plus, if you are manufacturing goods or rely on computers for employees to properly do their jobs, the efficiencies of your company will grind to a halt.

What happens next?

Even when the initial impact of a breach is over, other longer-term pernicious effects may affect your company negatively. These costs impact your business' rebuilding efforts indirectly and even years after the breach.

Damage control

This is one of the most extensive longer-term impacts of data breaches. A lot of victims and customers rightfully request compensation for the losses incurred from the business. They opt for legal recourse, even when the losses are not financially quantifiable.

Moreover, the cost of remediating and repairing the company website or database can be huge after a data breach. A large part of the whole remediation process involves altering employee behavior and business processes, both of which are time-consuming tasks.

Loss of intellectual property

Losing consumer data can be costly, but businesses can recover eventually. Unfortunately, the loss of intellectual property threatens the very existence of the business. Intellectual property is, after all, the heart of modern businesses, making up for 80 percent of a business' value.

As more news emerges regarding the effects of intellectual property loss on business, executives are starting to better align cyber-security measures with IP management. However, a lot of organizations still leave important assets fully exposed.

The damage dealt with the brand value of a business is not something that goes away anytime soon. Rather, companies that fail to respond fast to an incident may expect a decline in share price that normally lasts over 90 days.

Summary

Make it a priority to protect your operations from cyber threats. Even if it’s not possible to safeguard all aspects of your business, you can make it difficult for hackers and other malicious online entities to access your sensitive PII. If you’re yet to see the overall threat picture and have not taken steps to protect your business from catastrophic events, you are putting the growth of your business at risk. You need to take proper business decisions to guide your business to success.

About Us

"FileCloud is used by 1000s of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers."

A privately held software company, headquartered in Austin, Texas, USA. Our company offers two products – Tonido for consumers and FileCloud for businesses – used by millions of customers around the world, ranging from individuals to Global 2000 enterprises, educational institutions, and government organizations, and managed service providers.

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support"

Stewart

ℹ To read more about how FileCloud can help keep your information secure as it is shared, visit www.getfilecloud.com