WHY CLOUD SECURITY IS PARAMOUNT TO YOUR BUSINESS'S WELL-BEING

cogent infotech

THE FUTURE OF CLOUD SECURITY

Cloud security isn't some security fad that will soon drift into the digital abyss. With waves of companies now adopting cloud computing, it's glaringly evident that it is here to stay. But with novel technology comes new security risks.

Since 2013, there have been an astounding **3,776,738 records stolen via breaches every day.** With 95 percent of hacks occurring within just three industries - Government, Retail and Technology - now more than ever, businesses should be looking to shore up their cloud security.

Bolstering one's cloud security will have an extensive effect on one's business that goes beyond protecting against breaches.

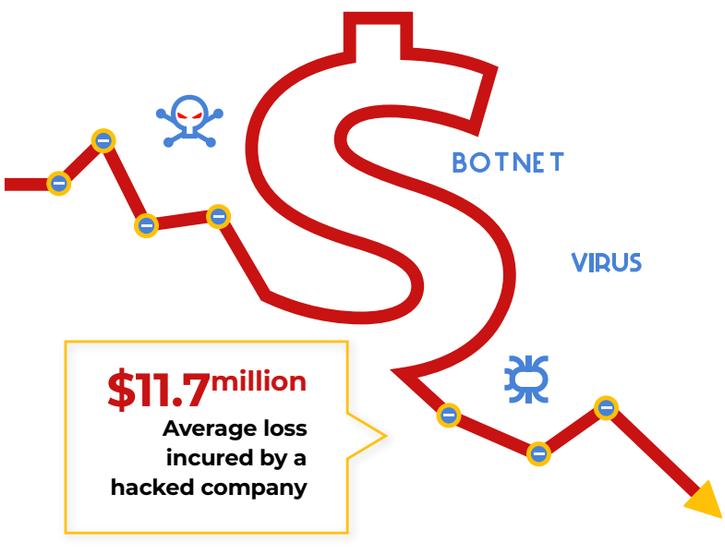
COMPANY REPUTATION

Once customers learn of a cyberattack, they will subsequently alter their opinion of the hacked company. A 2015 survey asked 39 organizations which aspect of being hacked was the worst.

A total of **16 of these organizations cited damage to company reputation as the worst by-product of the breach.**

Keeping data breaches under wraps would mitigate reputation damage. However, recent government policy requires that nearly all companies disclose data breaches. The most impactful way to protect your company reputation is to invest in preventative cloud security measures and train employees to employ effective security practices.

FINANCIAL LOSS

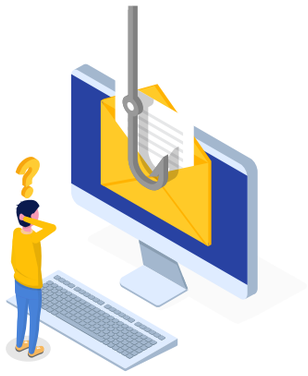


The average cost of cybercrime has significantly grown in the last five years. In 2017, **the average loss incurred by a company that had its data hacked was $11.7 million**. The primary financial loss comes from the need to pay exorbitant fees to third-party investigators and cybersecurity specialists to contain the attack, identify the source and to fortify cybersecurity to ensure that another attack doesn't occur. The frenzied state that an attack will leave a company can also **affect efficiency and lead to financial loss.**

cogent infotech

EMPLOYEE INEXPERIENCE

Employees are credited for making businesses tick. A manager doesn't need to think too long before knowing who to thank for a company's progress. However, it's these same employees that reveal themselves as security liabilities.



Phishing and social engineering attacks purpose of infiltrating a company's security by preying on an employee's negligence. **Adequate security training will turn employees into data guardians.**

DISCLOSING THAT YOU'VE BEEN BREACHED

Even the smallest of businesses operating within the healthcare and financial industries must reveal that they've been breached to their customers. Government regulatory bodies require that a certain level of disclosure be made not only to the public but in certain cases to the media as well. With some of the most prominent financial monoliths having been hacked in 2018 (Goldman Sachs, RBS, Sallie Mae) **any company in the financial sector, no matter how small, is susceptible to a breach.**

A cyberattack has far-reaching consequences that one can only combat with adequate cloud security. Traditional network security, where every piece of information was held in a data center and connected to a single network, is now an obsolete practice.

With Cogent Infotech navigating your company through the murky waters of cybersecurity, you will **receive cloud security-driven technology solutions that will assist you in your Digital transformation journey.**

To know more about cloud security solutions, connect with us on **digital@cogentinfo.com.**

cogent infotech