



The Cost of Doing Nothing

Not investing in cybersecurity could be your organization's most expensive mistake—and may ultimately ruin it.



INTRODUCTION

On July 19th, 2019, Capital One, one of the biggest banks in the U.S., suffered a massive data breach. A lone hacker managed to infiltrate Capital One's database and steal the personal information of more than 100 million customers and credit applicants in the United States and Canada.

The exposed data included customers' names, addresses, phone numbers, self-reported income, credit scores, and payment history. Also leaked were the Social Security numbers of more than 100,000 Americans and Social Insurance numbers of more than one million Canadians.

The fallout came quickly; less than 24 hours after the event, Capital One customers whose accounts were compromised filed a class-action lawsuit against the bank, accusing it of serious "security failures." Soon after the news broke, the company's stock was down almost 6% in premarket trading.

In August the following year, the courts found Capital One guilty of security negligence, slapping the company with an \$80 million fine. However, experts estimate that factoring in lost customer confidence, reduced earnings, and lowered share value, the total loss could be [billions of dollars](#).

Capital One's case is by no means unique; two years before Capital One's incident, Equifax, one of the largest consumer credit reporting agencies in the U.S., also suffered a data breach. The incident cost them about \$700 million to resolve—lawsuits included. However, the company's share price drop and post-breach damages resulted in [\\$4 billion being wiped off their market value](#).



AND IT'S NOT JUST BIG BUSINESSES EITHER

Of course, Equifax and Capital One are extreme cases, demonstrating just how damaging a security incident can be. But the costs of a data breach aren't exclusive to large businesses and organizations. Research shows that Small and Medium-Sized Businesses (SMBs) are also vulnerable to cyberattacks, if not more so.

Many believe that SMBs are too small to be attacked and that there is less value in their information. However, nothing could be further from the truth; cybercriminals know that SMBs have fewer resources to invest in security and training, making them easier targets for cybercrime.

The damages, however, can be colossal. If you own a small business and suffered a data breach that compromised 10,000 customer records, at \$150 per record—the average cost per compromised customer's Personally Identifiable Information (PII)—you could be looking at costs starting at \$1.5 million.

What's even more alarming is that [recent surveys](#) show that most SMBs estimate the cost of a data breach to be just \$10,000. However, data breaches are almost 15 times more expensive—the average cost for SMBs being \$149,000.

The fact is that cyberattacks are no longer a matter of *if* but rather *when*. Even a "minor" cybersecurity incident can have a devastating effect on your company's finances, reputation, and business continuity.

With cybercrime costing the world over [\\$1 trillion in damages last year](#), business leaders must understand the enormous risks and costs that come by not investing in their cybersecurity.

CYBERATTACKS ON SMBS



28%

of cyberattacks specifically target small businesses



76%

of SMBs experienced an attack in 2019



69%

of SMBs worldwide experienced cyberattacks that got past their security systems



HOW MUCH CAN A DATA BREACH COST YOUR COMPANY?

According to IBM and Ponemon Institute's 2020 "[Cost of a Data Breach](#)" report, the average total cost of a cybersecurity breach is **\$3,860,000**.

However, dozens of factors can inflate this figure:

Type of record compromised

Does your company have any Personally Identifiable Information (PII) of your customers or consumers? If you do, a data breach will cost you more.

The Ponemon study showed that customer PII is the **costliest type of data**, costing an average of \$150 per lost or stolen record.

1

The same Ponemon survey also discovered that customer PII was the type of data compromised most often—80% of data breaches globally involved customer PII.

Cost per record for other types of compromised data:

- Other corporate data (\$149)
- Intellectual property (\$147)
- Anonymized customer data (\$143)
- Employee PII (\$141)

2

Location

The location of your business and organization also affects the cost of a data breach. Organizations in the U.S. **have the highest average total cost at \$8.64 million per incidence**, followed by the Middle East at \$6.52 million.

In contrast, Latin American and Brazilian organizations have the lowest average total cost of mitigating a data breach at \$1.68 million and \$1.12 million, respectively.

3

Type of Industry

Industries with stricter regulatory requirements have higher average data breach costs. For instance, a data breach in the healthcare, energy, financial services, and pharmaceutical industries is significantly higher than less regulated sectors such as hospitality, media, and research.

Though the costs were lower for the public sector last year, cybercrime is on the rise. Government schools and agencies suffered a tide of ransomware attacks in recent months, leading to a proposed legislation that, once passed, would launch a [\\$500 million annual grant program](#).

Meanwhile, a recent survey reported that the education industry was the [hardest hit industry by ransomware in 2020](#), with cybercriminals targeting the wealth of student data in educational institutions.

Average data breach costs per industry:

- Healthcare: \$7.13 million
- Energy: \$6.39 million
- Financial: \$5.85 million
- Pharma: \$5.06 million
- Education: \$3.90 million
- Public: \$1.08 million



Organizational size

4

Generally, the bigger your company, the more costly a data breach incident will be. However, the Ponemon survey discovered that the mid-sized organizations (5,001-10,000 employees) had the highest average cost for a data breach.

Average total cost of a data breach by organizational size:

- Less than 500 employees: \$2.35 million
- 500 to 1,000 employees: \$2.53 million
- 1,001 to 5,000 employees: \$3.78 million
- 5,001 to 10,000 employees: \$4.72 million
- 10,001 to 25,000 employees: \$4.61 million
- More than 25,000 employees: \$4.25 million

Root cause

5

The Ponemon survey identified three root causes of a data breach; human error (23%), system glitch (25%), and malicious attacks (52%).

Out of these root causes, a data breach from a malicious attack is the most expensive, costing companies **\$4.27 million on average**—nearly \$1 million more than breaches caused by a system glitch or human error.

- Malicious attacks: \$4.27 million
- System glitch: \$3.38 million
- Human error: \$3.33 million

Destructive malware, ransomware, and malicious attacks

6

Damages from destructive malware (programs designed to destroy data in destructive/wiper-style attacks) were the most expensive, followed by ransomware attacks and the average data breach.

- Destructive malware: \$4.52 million
- Ransomware: \$4.44 million
- Average malicious attacks: \$4.27 million



BREAKING DOWN THE COST OF A CYBERATTACK

Although there's a tendency to focus on direct financial losses (such as ransom paid due to ransomware), the indirect costs of a data breach could be far more expensive. Worse still is that the effects of a cyberattack could affect an organization years after the incident—compounding the cost of the initial damage.

In this article, we explore the less considered costs of a cyberattack to give a clearer picture of just how expensive a cybersecurity incident can be.





Regulatory Fines

Compliance with regulatory bodies has become a top concern for executive boards these days, and for good reason—the fallout is expensive.

Mandates such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA) are there to ensure that non-compliance is a costly mistake for businesses and organizations.

Take the [CCPA](#), for instance; each time a business is found to have an intentional violation, they can be fined up to \$7,500, while unintentional violations can be fined \$2,500. At first glance, these may not seem like a lot until you realize that the violations stack up.

For instance, if a business's website uses third-party cookies without leveraging a cookie banner for awareness and opt-in, that organization could potentially be committing thousands or more violations per day. For high-traffic businesses, the fine could easily reach millions, if not more.



Operational Downtime

Businesses know that shutting down operations due to a cybersecurity incident will result in financial strain; however, few realize just how expensive this can be. The cost of business interruption associated with a cyberattack can often be **five to twenty times higher** than the direct costs from the attack itself.

For instance, in 2019, the average cost of downtime for SMBs was \$141,000. That's more than [20 times higher](#) than the average ransomware demand from SMBs from the same period (\$5,900).

According to Gartner, the average cost of Information Technology (IT) downtime is \$5,600 per minute or \$336,000 per hour. However, this could vary depending on your organization's IT reliance and business model; a separate study by McAfee revealed that 33% of survey respondents experienced an IT security incident resulting in a system downtime that cost them [between \\$100,000 and \\$500,000](#).



Reputational Damage

While assigning an average monetary value to reputational damage can be challenging, its impact is undeniable.

Firstly, there's the irreversible reputation damage on the information security leadership; for example, in 2016, Uber suffered a data breach that compromised the personal information of 57 million users. A year later, the ride-hailing firm fired its chief security officer, Joe Sullivan, and deputy Craig Clark for their [roles in the breach for attempting to cover it up](#).

Secondly, there is the reputational damage to the company. Compromised customer data invariably causes a loss of customer confidence, resulting in brand-bashing, diminished loyalty and trust, and preference for your competitors' services.

For publicly traded companies, this could mean plummeting shares and an overall decrease in company value. Add to that the costs of regaining your customers' trust (which usually involves free services and PR campaigns to demonstrate how you improved your security post-breach), and you'll start to see just how devastating a data breach fallout can be.

The Equifax data breach perfectly illustrates this. Within the first week of their breach, Equifax lost four billion dollars in stock market value. The costs of damage mitigation post-breach totalled an additional \$439 million by the end of 2017.

To regain customer confidence, Equifax offered 147 million customers free credit monitoring services for one year and a waiver of the requirement that all disputes be settled through arbitration. However, a year later, a survey showed that [28.4% of their customers](#) still haven't forgiven the company.

Equifax was court-ordered to spend \$1 billion in enhancing their cybersecurity under court oversight to top it all off.





Legal Costs

It's best practice for companies to retain counsel, especially during a cybersecurity incident. On average, the hourly attorney rates hover around \$1,000 and can quickly snowball, especially when engaging a legal team to handle a complex case. More significantly, your legal costs can grow exponentially, especially if your company was involved in a class action lawsuit.

In the case of Home Depot, the retailer was taken to court over its 2014 credit card data breach incident, which affected 56 million customers. A federal judge later ordered Home Depot to pay \$15.3 million in fees and expenses to lawyers who litigated the class action case.



HOW TO PROPERLY INVEST IN CYBERSECURITY

Organizations must start viewing cybersecurity as an investment rather than a cost. The potential savings are significant, but more importantly, investing in cybersecurity ensures that your business continues to grow and operate.

Consider investing in these areas to improve your organization's overall cybersecurity posture:



Train your employees

An organization's cybersecurity relies on three main pillars: people, processes, and technology. Unfortunately, people will always be the weakest link.

A recent report revealed that human error led to increased cybersecurity risk and challenges for [80% of businesses during the pandemic](#), proving that even the most detailed, security-forward processes and top-notch technical solutions won't work without empowered staff.

Annual cybersecurity training simply isn't enough—organizations must develop a culture of security. For example, you could have your employees complete regular monthly modules, to ensure that they're aware of the latest trends in cybercrime. You could also run frequent phishing campaigns and offer incentives for staff who successfully report malicious emails.

Improving cybersecurity awareness and overall knowledge of your workforce will significantly elevate your long-term security posture.






Practice Incident Response Procedures

According to IBM and the Ponemon's Institute's 2020 "[Cost of a Data Breach](#)" report, an organization that tested their Incident Response Plan saved approximately \$2 million on a data breach incident compared to those that didn't.

Everyone in your organization must know what to do in the event of a data breach. Schedule regular drills and identify weaknesses in processes so you can improve them. Update your response plan regularly and ensure that someone is continuously improving it.

Run your plan through the following checklist:

 Is your plan clear on reporting requirements?	 Does your company have cybersecurity insurance?	 Are the details of the relevant contacts updated?	 Has your plan been updated in the past six months?
--	--	--	---

Recognize that a data breach event is an incredibly high-pressured and stressful situation. Regulatory bodies such as GDPR require that companies report data security incidents within 72 hours of discovery, and without a detailed, updated plan in place, your company is headed for disaster.

Having a proper incident response plan means the people with the right skill sets and experience will be able to handle the situation and successfully contain and remediate the threat.



Understand Your Regulatory Requirements

As a business, it's your responsibility to know what regulatory requirements you need to comply with. Claiming ignorance will not save you from the hefty fines from regulatory bodies such as HIPAA, CCPA, and GDPR.

If your business stores large amounts of customer's Personally Identifiable Information (PII) or Personal Health Information (PHI), it may be worth hiring a Chief Privacy Officer. This individual would be responsible for ensuring that customer data is appropriately secured, and that the business complies with all regulatory requirements.



Test for weaknesses in your security

Like any sound defense system, it's crucial to know what and where your weaknesses are. It's good practice to conduct a yearly cybersecurity risk assessment and check for possible flaws among your employees, processes, and technologies.

Hire a qualified external vendor with the knowledge and skills to conduct an in-depth cyber risk assessment that meets industry standards. Ideally, your cybersecurity should measure up to frameworks set by the National Institute of Standards and Technology (NIST) and Cybersecurity Framework (CSF).

Having identified the risks, a qualified vendor should provide an in-depth recommendation on fully remitting or mitigating the associated risks. Typically, findings and recommendations come with a strategic implementation roadmap that will tremendously improve your overall security posture.



Hire an expert

Even the largest organizations will find it challenging to handle cybersecurity on their own. Compliance regulations may require network, IT infrastructure, and cloud services monitoring 24/7 across all endpoints, firewalls, and access points—which is, frankly, beyond the capabilities of most IT teams.

According to Ponemon, one of the best ways to [minimize the impact of a cyberattack](#) is by hiring a managed security service provider (MSSP). A qualified MSSP would know the best practices and industry trends of the moment and offer insights into what's currently working in the field.

CONCLUSION

A data breach incident is not just expensive; it's *a lot more* expensive than what most businesses realize. While the upfront costs of proactively investing in your cybersecurity can be a strain on your budget, you'll most certainly save more money in the long run.

When businesses and organizations don't sufficiently invest in cybersecurity, the risks of a successful cyberattack—and subsequently the cost of damages—increases exponentially. Even with multiple internal resources, it's a good idea to place a specialized cybersecurity responder on retainer.

Partnering with a good MSSP will ensure compliance with cybersecurity-first processes and practices and even support the training of staff on the secure handling of sensitive data. A good MSSP would also help put a response team together, initiate immediate remediation in the event of an attack, get systems back online as quickly as possible, support negotiations, and help prevent future incidents.

As a tech-agnostic MSSP, Digital Hands improves your business' cybersecurity with a unique "composable security" platform that can be customized to your organization's specific needs.



Partnering with a good MSSP will ensure compliance with cybersecurity-first processes and practices and even support the training of staff on the secure handling of sensitive data.



ABOUT DIGITAL HANDS

Digital Hands is a trusted, award-winning cybersecurity leader with extensive security expertise offering advanced protection, detection, and remediation services. Digital Hands' Composable Security Model optimizes legacy security infrastructure while augmenting with today's latest security solutions to safeguard your organization against ever-present cybersecurity threats around the clock, anywhere in the world. To learn more, please visit www.digitalhands.com.





www.digitalhands.com

(855) 511-5114

4211 West Boy Scout Boulevard Suite, 700 Tampa, Florida 33607

sales@digitalhands.com