CLARUS
TECH PARTNERS

Cybersecurity and Data Regulatory Compliance Cost Impacts

Clarus Tech Partners

CONFIDENTIAL AND PROPRIETARY

How Much Does a Data Breach Cost for a Small-Medium Sized Business?

A single cyber attack could directly impact your business' budget—the average dollar amount is $38,000 per attack and the cost of cyber attacks could soar to $55,000 and above. Keep in mind that this doesn't include the indirect costs you may experience.

These numbers come from the time in productivity that a security breach will cost your company in addition to the services you'll need to try and fix the security breach. These professional services could range from IT consultants to lawyers and public relations officials. The cost of cyber attacks includes the *time and resources you'll spend trying to deal with such an attack—all of which impact the success of your business.*

Large businesses can expect to pay nearly 15 times more than small businesses when it comes to the cost of cyber attacks. This means that even on the lower end of $38,000 for small businesses, large businesses can expect to pay $570,000 and even more. On average, a large business will pay $824,750 for cyber attacks and this number could go as high as $2 million.

What is the Average Cost of a Data Breach?

In 2022, the average total cost of a data breach increased by 2.6% to $4.35 million, the highest ever recorded. From 2020, the average cost has increased by 12.7%, from $3.86 million. Moreover, costs were even higher when remote working was presumed to be a factor in causing the breach, increasing to $4.99 million.

The research shows that faster incident response times were associated with substantially lower costs, with a cost savings of over 25% if a breach was contained in less than 200 days.

- Data breaches commonly involve financial information like credit card or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property. Other terms for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage, or a data spill.

- Frequency and cost of various initial attack vectors including the top four most common: compromised credentials (19% of breaches), phishing (16%), cloud misconfigurations (15%), and vulnerability in third-party software (13%).

Why Aren't Businesses Aware of the Danger?

In small data breaches, the costs, disruption, and reputational damage are all greater than the small business ever anticipated. Businesses often mistakenly assume "It won't happen to me" or "This is probably covered somewhere in my insurance." But 83% of the organizations studied in the 2022 IBM Security Cost of Data Breach report, experienced at least 1 data breach. For only 17% of those organizations was this their first data breach.

Businesses are responsible for any damages associated with a third-party data breach. This type of event can be very damaging to small companies and can put many of them out of business because they often don't have the financial resources to manage and pay for a breach. Burying your head in the sand isn't a good approach, as a cyber attack and non-regulatory compliance can be incredibly costly.

Check out these figures:

How Much Does a Data Breach Cost a Business?

For a small or medium-sized business (SMB), the average cost of a breach is $108,000, as stated above. Meanwhile, the cost for enterprises (businesses with more than 1000 employees) has risen to $1.41 million, up from $1.23 million the previous year. The financial damage will vary significantly depending on the size of the company and the nature of the breach.

Ransomware Attacks

According to IBM, the average bill for recovering from a ransomware attack, including forensics investigations, downtime, notifying regulators and customers, people hours, systems and networks costs, lost opportunities, etc. was $4.54 million in 2022, not including the ransom itself.

How Much Does a Forensic Investigation Cost?

Forensic investigations can be extremely costly. The cost will depend on the size of your organization and the larger your organization, the more data you likely have that will need to be examined.

Costs of a forensic investigation range between $50K to more than $500K. But a forensic investigation is only a portion of the costs you will probably incur in a data breach. Other costs include:

- Merchant processor compromise fines: $5,000 – $50,000
- Card brand compromise fees: $5,000 – $5,000,000+
- Onsite QSA assessments following the breach: $20,000 – $100,000
- Free credit monitoring for affected individuals: $10 – $30/card
- Card re-issuance penalties: $3 – $10 per card (this could be included in card brand compromise fees)
- Security updates: $15,000+
- Attorney fees: $5,000+
- Breach notification costs: $1,000+
- Technology repairs: $5,000+
- Compliance regulator reporting and penalties: Varies
- Possible civil litigation: Varies
- Loss of consumer confidence: often businesses lose 40% of customers after a breach

What are Possible Fines for Non-Compliance on Data Breach and Consumer Protection Regulations?

Some examples of fines include:

- The CPRA is an update to California's consumer protection act (CCPA), and it's the strongest such law in the United States to date. Even organizations that are not headquartered in California but have business in the state are required to comply with the CPRA. Collecting data on any individual in California can demand data compliance.
    - Intentional violations are fined $7,500 per record. This can add up very quickly since violations usually occur across large databases and not just to individuals. Intentional violations can include failing to notify consumers about data collection, failing to respond to data requests or deletion requests, or selling data after a client has specifically requested the company not to do so.
    - Unintentional violations cost $2,500 per record. This is usually applied in breaches where adequate security measures were in place.

- Canada's Personal Information Protection and Electronic Documents Act, or PIPEDA, If you collect data on Canadian citizens, you may be subject to PIPEDA fines if a breach occurs. Breaches must be reported immediately, and you have to keep records of the incident for at least two years. Any attempt to cover up a breach, stymie investigations, or even punish employees who act according to PIPEDA rules can lead to fines of up to $100,000 CAD.

- The Health Insurance Portability and Accountability Act is one of the oldest US federal privacy laws. Depending on the tier, fines can range from $100 to $50,000 per incident, with a maximum of $1.5 million.

- Under the European Union's General Data Protection Regulation (GDPR), organizations can face fines up to €20 million ($22,885,000 USD) or 4% Adjusted Gross Revenue, whichever is larger. Remember that you do not need to be based in Europe for these rules to apply to your business. Just possessing data on European citizens is enough.

- Gramm-Leach Bliley Act (GLBA) which mainly covers financial organizations, can result in fines of up to $100,000 for each violation.

- In addition to this small sample of laws and regulations, there are many more data breach, consumer and data privacy regulations in the U.S. and around the globe.

At Clarus Tech Partners, we have expertise in cybersecurity, data protection, risk management, data privacy, and regulatory compliance to address your cybersecurity risks and compliance requirements in the U.S., Europe, and globally.

Clarus Tech Partners
Email: Info@ClarusTechPartners.com | **Phone:** 646-926-3850 | **Website:** ClarusTechPartners.com