PKWARE

pkware.com

How Much Can You Lose in A Cyber Attack?

The Ripple Effect of A Data Breach

2022

Contents

Introduction

Despite global efforts, every year cyber-attack statistics grow larger and more threatening. In 2021 alone, the average number of cyberattacks and data breaches increased by 15.1 percent over 2020. This sharp increase should prompt organizations to consider when—not if—they will be attacked and prepare accordingly. But in order to do so, businesses need something that has been lacking in most cybersecurity conversations up to this point: a deeper understanding of both the risks and the true costs of a data breach.

As data breaches are reported publicly, details tend to include the number of individuals who were impacted, the dollar amount of a ransom demand, or how much the cyber attacker is selling the information for on the dark web. Yet costs and the associated business fallout goes beyond just this first layer of the initial impact.

According to IBM's most recent Cost of a Data Breach Report, the global average total cost of a data breach has recently increased 10 percent to $4.24 million. When ransomware is involved, the cost increases to $4.62 million, which includes escalation, notification, lost business, and response cost. It does not include the cost of the ransom, which typically averages around $150,000. Looking at data breach statistics from the United States alone, the cost of a data breach more than doubles to $9.05 million. While remote work has become the norm over the past two years, it also increases the cost of a data breach by $1.07 million.

The global average total cost of a data breach has increased to $4.24 million. When ransomware is involved, the cost increases to $4.62 million.

We often define data breaches in dollar amounts, but it's not simply a cost problem. Nor are breaches just about the data. Rather, it's about an organization's ability to continue producing and selling their products and/or services.

Security is, therefore, a business problem.

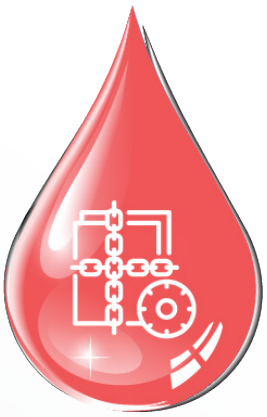
Initial Impact

The initial impact of a data breach—whether it originates internally or externally—is likely to be first felt in the day-to-day processes of doing business via an inability to access the critical information necessary to do business. The immediate business "cost" thereafter may depend on what "doing business" means to the organization and how that then results in external impacts.

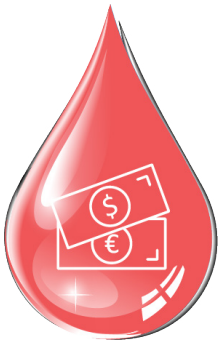
For example, when hackers gained entry to the Colonial Pipeline Co. networks in late April 2021, the organization was forced to shut down the largest fuel pipeline in the US a week later in order to contain the attack. During the six-day pipeline shutdown, panicked East Coast residents flocked to gas stations to hoard fuel, driving the cost to $3 a gallon for the first time in years and ultimately resulting in many local gas shortages. Seventeen states and Washington, D.C. ended up declaring a state of emergency.

Despite Health Insurance Portability and Accountability Act (HIPAA) healthcare data compliance measures having been in place since 1996, hacking and healthcare data breaches are recently on the rise, and experts predict that trend will continue. Beyond the inability to access data or the ruinous consequences of having patients' private data available publicly, healthcare data breaches have real life and death consequences as well: In 2019, a study found that for every 10,000 heart attacks at a hospital that was experiencing a cyber breach, there were approximately 36 additional deaths over and above the typical heart attack fatality rate.

Even when looking at the most commonly reported information for most data breaches—which is number of records impacted—initial monetary costs add up quickly. The top type of compromised record is customer personally identifiable information (PII), which costs around $180 per lost or stolen record. Following logically, the larger the breach, the bigger the price tag: Breaches of 50 – 60 million records are almost one hundred times more expensive than 1,000 – 100,000 records.



The Ripple Effect: Systems, Brand, and People



There's more to a data breach, though, and the after effects can reach far and wide. Lesser seen impact can include the cost of remediation, revenue loss, reputational harm, national security, even as reported above, human life. The ripple effect of indirect costs—monetary and otherwise—can impact a company's bottom line for years.

Breaking a data breach into accounting terms, companies can expect to segment the resolution process into four cost centers: Detection and Escalation, Notification, Post-Breach Response, and Lost Business.

Detection and Escalation

This first cost center is most often involved in the initial "pebble drop" cost, encompassing all the activities that enable a company to reasonably detect the data breach, and amounting to approximately 29 percent of the total cost of the data breach. Based on the global average of $4.24 million, the price tag hovers at $1.24 million.

Notification

Many data compliance regulations such as HIPAA, the EU's General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) require that customers whose data has been impacted by a breach be notified within a set period of time. Failure to do so results in significant fines for the organization. Even without the line item of a notification fine, the activities that ultimately allow the company to notify those impacted as well as data protection regulators and other third parties accounts for six percent ($0.27 million) of the total cost of the breach. Any organization that does not notify their customers within the expected parameters can expect to see additional fines down the line.

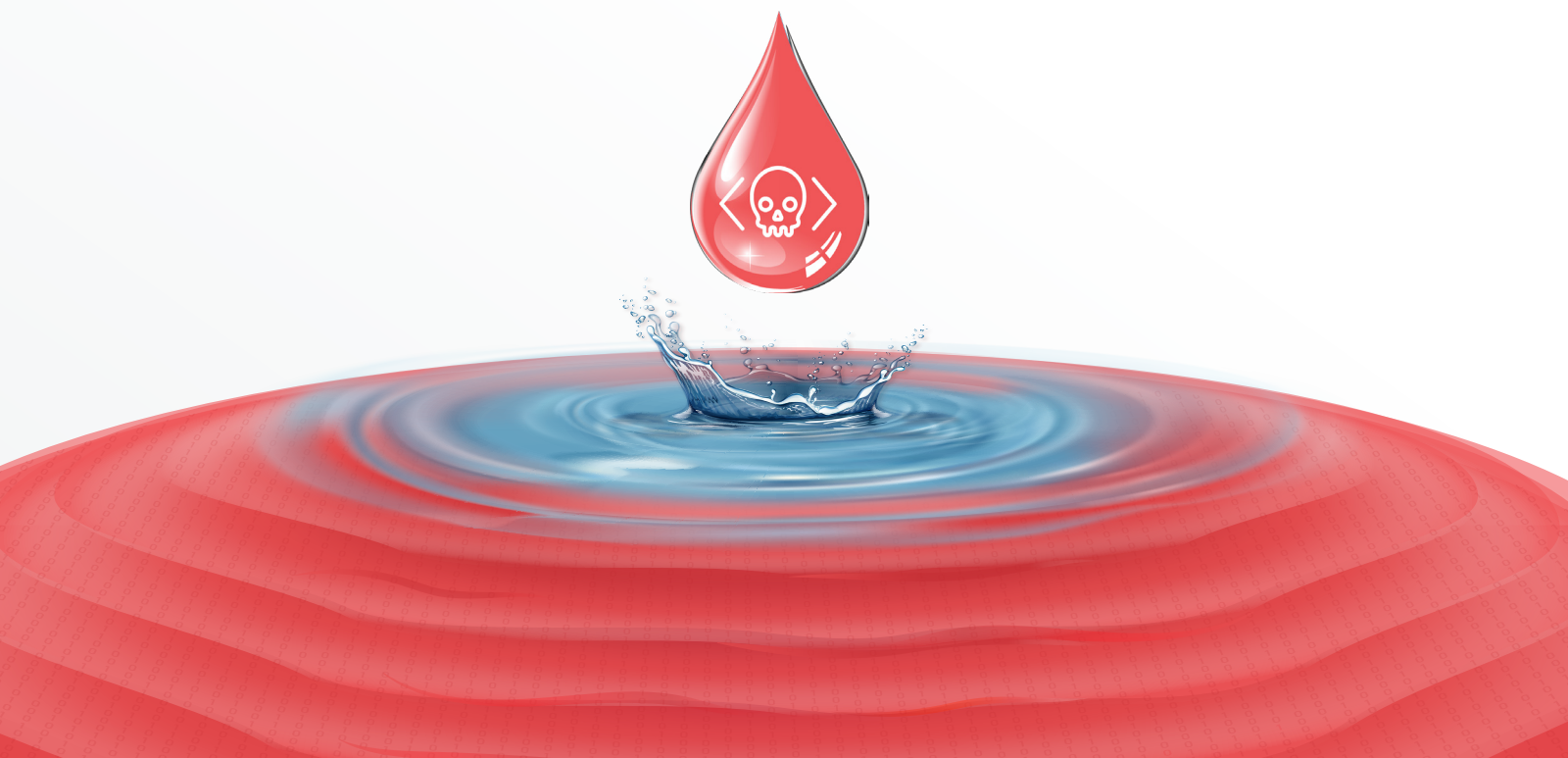
Post-Breach Response

It's not enough to simply notify customers of a data breach. With brand reputation now at risk, it's crucial to provide activities that will help the victims of the breach communicate with the company, and remedy the issues as much as possible with victims and regulators. These actions could include credit monitoring, product discounts, legal costs, even the cost of time needed to issue new accounts or cards. This cost center carries a larger percentage of the total average monetary cost of a breach at 27 percent, or $1.14 million.

Regulatory fines for data breaches also typically fall into the Post-Breach Response cost center. These are the top factors for amplifying the data breach costs. To compound the issue, these costs aren't necessarily incurred at the time the breach is discovered or remedied—20 percent of costs in highly regulated industries are incurred as far out as two years after the breach.

Lost Business

The largest share of the average cost at 38 percent ($1.59 million), this cost center accounts for all activities enacted to minimize customer attrition, disruption of business, and revenue loss. This includes replacing revenue lost during system downtime, as well as detractors such as reputation loss. Not only will established customers leave—breached organizations may lose up to a third of their existing customer base—media and word of mouth may make it difficult to attract new customers depending on the depth and severity of the data breach. Data security notwithstanding, it is already estimated to cost five times as much to attract a new customer than to keep an existing one. A publicized breach could increase that price tag significantly.



These four cost centers represent distinct areas with measurable dollar amounts tied to them, costs that reveal layer after layer as teams work to control and resolve a data breach. But beyond the dollar amounts, companies must also consider the cost of time as they work to return to "normal."

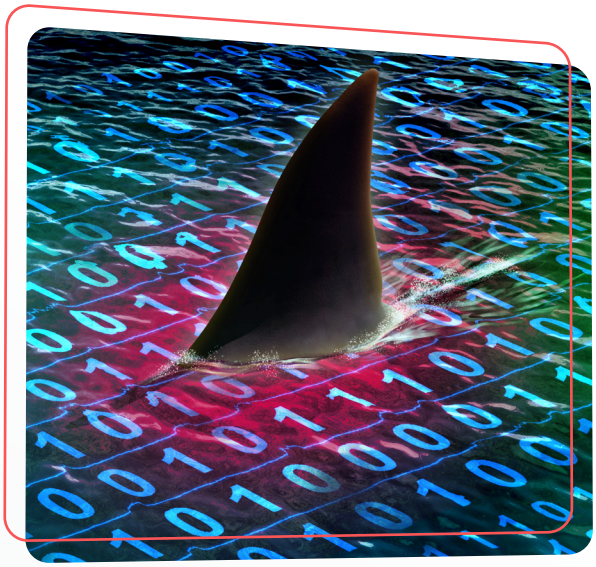
It follows logic that the longer a breach goes on, the more impact it has on the business. According to one McAfee survey of 500 senior IT decision makers, they believed it took an average of only 10 hours to detect a data breach. Studies and anecdotal evidence suggest otherwise. The Verizon Data Breach Investigation Report found that 66 percent of breaches weren't found for months or even years. According to IBM, it takes on average 287 days to identify and contain a data breach, the breakdown of which averages 212 days to identify and 75 days to contain the breach. This means that if a breach occurred on January 1, it would not be fully contained until October 14. The post-COVID shift to more remote and hybrid work only exacerbates this issue: Organizations that have a workforce made of more than 50% remote employees averaged a full 306 days to contain the breach—235 days to identify, and 81 to contain. If their breach began on January 1, it would span all the way through November 12 before being fully contained.

One contributing factor to the length of time, according to expert Jonathan Weber of Marathon Studios, could be that many attacks do not offer external disruption to essential services. "Once the initial leak event has passed, there are little or no indicators of the breach until the hackers return or the data surfaces elsewhere," he reported to Dark Reading. A recent study of data breaches by Positive Technologies found that external attackers can breach an organization's network perimeter and gain access to local network resource in 93 percent of cases. Once the network perimeter is breached, the research reveals it takes an average of only two days to penetrate the internal network. Without accurate visibility into systems and networks and the inevitable cybersecurity blind spots, organizations don't know that an event is even happening. The same lack of visibility into data that allows attackers time to infiltrate and attack networks in the first place can make those same attacks extremely difficult to identify and resolve in a timely manner. Meanwhile, the effects of the breach continue to ripple outward.

Attackers can breach a network perimeter 93% of the time, penetrating the internal network next within 48 hours.

The Difference of Protection

In all fairness, cyber attackers have spent considerable time and resource to develop cyberattack methods that evade detection. Which means a focus on complete attack prevention may be unattainable—or if attainable, not sustainable for very long. Cyber criminals are becoming increasingly organized, with increasingly sophisticated attack methods. For most organizations, this means it's less a question of *if* a cyber-attack happens, but *when*. Adopting this approach adds an additional layer of protection beyond boundary control aimed at keeping threat actors out of your data, and begins including the extra measure of protection of making any data obtained unusable to anyone outside the organization.



First, organizations that use security AI and automation experienced on average an 80 percent reduction in cost of breach, largely due to their ability to more quickly identify and contain the breach. Organizations with fully deployed security AI and automate averaged 247 days total to identify (184 days) and contain (63 days) a breach. Using the same timelines referenced earlier, that puts a data breach that occurred on January 1 at full resolution by September 4.

While a shortened time to resolution certainly reduces the ripple effects and overall costs of a data breach, other protection methods can mitigate issues by ensuring that data remains in a state that renders it unusable to hackers and threat actors. For example, IBM's report found that high standard encryption was a top mitigating cost factor. Without decryption capabilities, encrypted data is worthless. Holding the encrypted data for ransom carries no weight without the option to decrypt what the files contain and release the sensitive information publicly. While customers and data compliance regulators must be notified of the breach, consumers may yet retain confidence in the business despite the breach if they know their data remains protected and inaccessible even in the wrong hands.

Other security tools can also come into play at keeping the ripple effects of a data breach to a minimum. Recall that companies with remote workers saw data breach costs increase by $1.07 million; unified endpoint management is identified as a solution for protecting and monitoring endpoints and remote employees. And with many businesses using multiple systems to accomplish their day-to-day business activities, security tools that can share data across disparate systems can also play a key role in minimizing the effect of a data breach.

Increase Visibility and Plan for Failure

The complexity of today's cyber environments—from hybrid environments spread across locations and teams to remote and hybrid work—all but guarantees the inevitability of a data breach. Navigating this inevitability means shifting focus from breach prevention to breach management. Essentially, cybersecurity teams should plan for failure: Assume your organization will at some point suffer a breach and put measures in place (automation, encryption, etc.) that can limit the widespread effects.

Reducing the impact and ripple effect of a data breach starts with increasing the level of visibility into networks, cloud services, and endpoints. Surveyed IT professionals reported their organizations have, on average, 750 endpoints in use on any given day. That alone can feel like an overwhelming number of places for data to hide, but then factor in servers, cloud, data repositories, and data lakes, and security teams face an enormous challenge in finding and protecting data everywhere it is stored, used, and sent. The recent State of Data Security 2022 Report found that only 8 percent of organizations could confidently find every piece of sensitive or critical data across their environments. Which means that 92 percent of organizations are still looking for their sensitive data, or may only know where it was stored after the environment has been attacked and the data stolen.

At PKWARE, we understand the enormity of what you're facing with data protection. We've spent the last four decades growing our data protection solutions alongside the ever-increasing volumes of data that need protecting. As one of the industry's most experienced data security companies, we have the proficiency, depth, and breadth to discover, secure, and protect sensitive data wherever it lives and moves to provide that critical layer of protection and minimize the threat—and cost—of a data breach.

Conclusion

The impact of a data breach will be felt far beyond just the theft of or inability to access sensitive and private data. The ability of a business to do what a business does—produce and sell their products and services under a trusted brand—also hangs in the balance, and each ripple felt after a data breach comes with a price tag.

Data security is a business problem that must be approached and solved that way, too, in order for businesses to withstand the inevitability of a breach attempt and minimize the far-reaching ripple effects of a sensitive data breach.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

Enterprise-Wide Policy Management

PK Protect provides a point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification, and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion

BOOK A DEMO

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204